C.1 BACKGROUND

The Continuous Diagnostics and Mitigation (CDM) program is a dynamic approach to fortifying the cybersecurity of Government networks and systems. As threats to the nation's information security continue to emerge, Government leaders recognize the need for a modified approach to protecting the Government's cyber infrastructure. The CDM Program enables DHS, Federal Agencies, and state, local, regional, and tribal governments to enhance and further automate their existing continuous network monitoring capabilities, compare and analyze critical cybersecurity-related information, and enhance risk-based decision making at the Agency and Federal enterprise level. The CDM Program benefits participating Agencies by helping to identify information security risks on an ongoing basis so that Agencies can rapidly detect and then respond to information security events.

Congress established the CDM Program to provide adequate, risk-based, and cost-effective cybersecurity and more efficiently allocate cybersecurity resources. The CDM Program provides Federal Departments and Agencies with capabilities and tools that identify cybersecurity risks on an ongoing basis, prioritize these risks based upon potential impacts, and enable cybersecurity personnel to mitigate the most significant problems first.

Starting in January 2013, DHS (operating on behalf of the participating Agencies) provided tools/sensors and services to execute Phase 1 of the CDM Program, which implemented the CDM Solution at each Agency in this TO. Beginning in June 2016, DHS provided tools/sensors and services to participating Agencies to execute Phase 2 of the CDM Program.

The CDM Program is organized by phases as identified below in Diagram 1: CDM Phases.

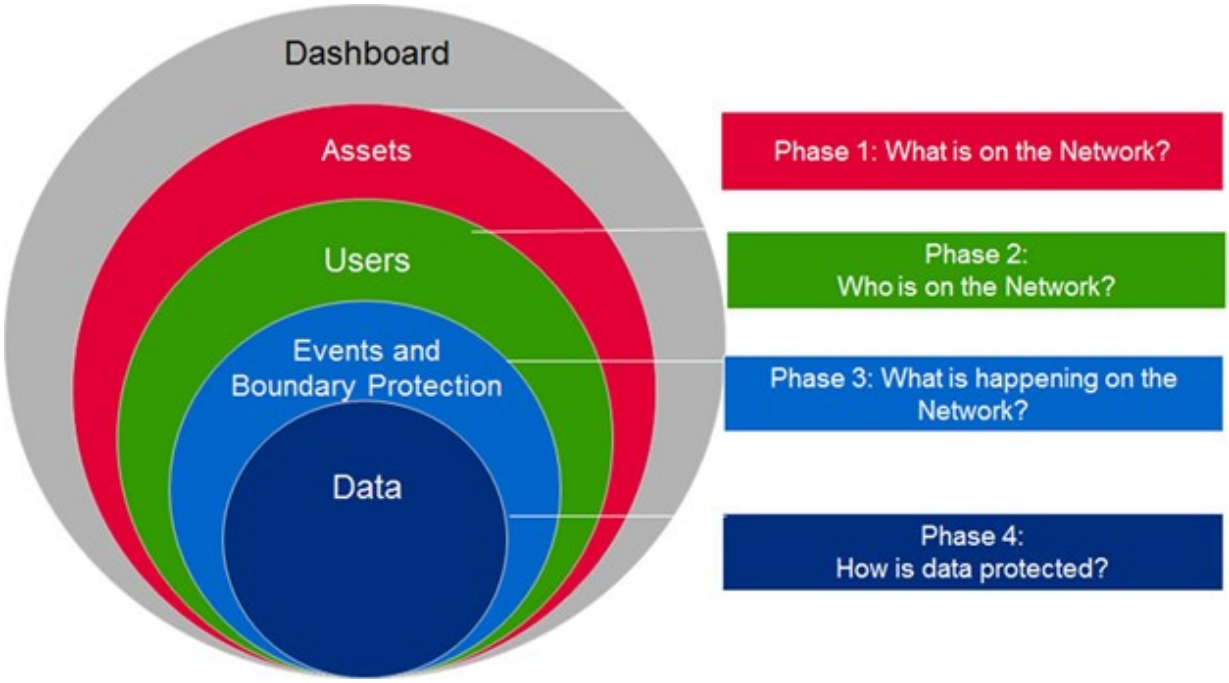

Diagram 1: CDM Phases

C.1.1 PURPOSE

The purpose of this TO is to resolve CDM capability gaps, enhance existing CDM capabilities, introduce new CDM capabilities, and provide support to the CDM Solution of participating Agencies, leading to a strengthening of their overall cybersecurity posture. The CDM Solution includes CDM approved products, configured to reflect the DHS CDM Program priorities and Agency policies as appropriate, that implements a common set of capabilities and enable increased risk-reduction and alignment with Agency risk tolerance.

C.1.2 DHS CDM PROGRAM MISSION

The CDM Program is managed within the DHS National Protection and Programs Directorate, (NPPD)/Office of Cybersecurity and Communications (CS&C)/Network Security Deployment (NSD) Division, responsible for enhancing the security, resilience, and reliability of the Nation's cyber and communications infrastructure. The DHS CDM Program mission is to safeguard and secure cyberspace in an environment where the threat of cyber-attack is continuously growing and evolving. The CDM Program defends the United States (U.S.) Federal Information Technology (IT) networks from cybersecurity threats by providing continuous monitoring sensors (tools), diagnosis, mitigation tools, and associated services to strengthen the security posture of Government networks. DHS has been given the authority and Federal funding to implement the CDM Program to ensure that the approach to continuous monitoring is consistent, meets a common set of capabilities, and leverages centralized acquisition to improve the speed of procurement and achieve significant cost savings by consolidating like Federal requirements into "buying groups." This TO is intended to achieve those objectives.

C.2 SCOPE

The scope of this TO is to provide support for all phases of the CDM Program and implement a common set of CDM capabilities across Federal Agencies. Within scope of this TO, the contractor will be required to:

a. Provision Agencies with CDM approved products, supporting ancillary products, and providing the associated services to the participating Agencies.
b. Fill existing gaps in Agency CDM Solutions to achieve a common set of capabilities.
c. Provide Operating and maintaining (O&M) the existing CDM Solution, while continuing to enhance and refresh CDM approved products, as appropriate.
d. Plan for Agency support of provisioning, configuring, operating, testing, and managing CDM tools, sensors, Agency-level dashboards, and data feeds as well as support for the CDM Solution's governance.
e. Develop, integrate, operate, and maintain the capability for CDM-approved products to report information to the Agency-level CDM Agency Dashboard.
f. Design, build, deploy, and operate the CDM Solution for component offices of the participating agencies that opt-in to the CDM Program.
g. Provide Agency-specific training for the CDM Solution, the Agency CDM Dashboard, and CDM governance support.

The performance of this TO is primarily at the contractor's facility. However, testing and validation efforts may require performance at Government facilities. The contractor's facility shall include spaces suitable for a development and test facility and support classified IT storage.

C.2.1 Supported Agencies

This TO will support the DHS CDM Program Management Office (PMO) by providing and/or enhancing the CDM Solution at the following Federal Agencies and their components, hereafter referred to as the Group E Agencies:

a. Department of Education (ED)
b. Department of Housing and Urban Development (HUD)
c. Department of Housing and Urban Development Office of Inspector General (HUD OIG)
d. Environmental Protection Agency (EPA)
e. Federal Deposit Insurance Corporation (FDIC)
f. Nuclear Regulatory Commission (NRC)
g. National Science Foundation (NSF)
h. Securities and Exchange Commission (SEC)
i. Small Business Administration (SBA)

C.3 OBJECTIVES

The objective of this TO is to operate and enhance the existing Group E CDM Solution. In compliance with applicable standards, this objective will be accomplished, through detection improvement and analysis of IT security events, and in cooperation with the DHS CDM PMO and the Group E end users.

Additional CDM Program objectives for the TO are to:

a. Reduce Agency threat surface through strengthening cybersecurity of Agency IT assets.
b. Achieve the most advantageous cost and price discounts while provisioning Agencies with CDM tools and capabilities.
c. Deliver flexible services that can accommodate dynamic cyber environments.
d. Timely completion of work to ensure delivered CDM capabilities are fully implemented at receiving Agencies.
e. Promote transparent and effective communications that accurately present status to CDM stakeholders.
f. Provide accurate reporting of Agency environments while achieving successful governance of Agency cybersecurity programs.

C.4 CDM CURRENT AND FUTURE STATES

CDM enables activities designed to strengthen the cybersecurity posture of the Federal civilian .gov networks. Specifically, the tools and sensors and associated services benefit the CDM Program by:

a. Simplifying the security authorization process by helping to automate security assessments.
b. Monitoring and reporting continuous system security status to Agency cybersecurity personnel via the Agency CDM Dashboard.
c. Providing specific details to help prioritize remediation efforts.
d. Allowing system owners, risk managers, authorizing officials, and other stakeholders to make better risk-management decisions.
e. Automating reporting of the security posture of Agency IT assets to the Federal Dashboard, thereby reducing the requirement for manual reporting.

The remainder of **Section C.4** summarizes the CDM Current State, CDM Desired Future State, and CDM Technical Capabilities. Where there is a perceived conflict between **Section C.4** and the CDM Technical Capabilities Requirements Documents, Volumes 1 and 2 (**Section J, Attachments Y.1 and Y.2**), the CDM Technical Capabilities Requirements Documents will take precedence.

C.4.1 CDM CURRENT STATE

An Agency-specific CDM Solution is currently operating on the Agencies' networks with diverse IT environments. The CDM Solution maintains a degree of consistency across the Group E Agencies by leveraging a similar set of Commercial Off-the-Shelf (COTS) tools. These tools have been reviewed by the DHS CDM PMO to identify that they meet the capabilities of, or in conjunction meet, the requirements specified in CDM Technical Capabilities Requirements Document, Volumes 1 and 2 (**Section J, Attachments Y.1 and Y.2**). A list of approved CDM tools is maintained by the DHS CDM PMO as the Approved Product List (APL) and is located at www.gsa.gov/CDM.

CDM approved and supporting ancillary products currently in use at the Agencies, as well as high-level IT and network infrastructure descriptions for each Agency supported by this TO, are identified in the Agency-specific IT/Network Environment Summary Information provided by the Government in the Electronic Reading Room (eRR). The Government desires that the contractor leverage any existing Agency investments when developing a solution for any CDM capability enhancement or new integration.

Two of the supported agencies, FDIC and SEC, have received limited Phase 1 and 2 support through the CDM Program. The activation of support for FDIC and SEC may be addressed by a Request for Service (RFS) post-award.

The CDM system architecture, shown below in **Diagram 2** – CDM Architecture, illustrates the CDM Full Operating Capabilities (FOC) vision once it has been implemented within the Group E Agencies.

a. Area A is the location for tools and sensors that, together, provide the coverage of the

CDM Capabilities.

b. Area B is the integration point solution that supports the required operational control points for the CDM Solution.
c. Area C is the Agency CDM Dashboard(s) that integrates into the Agency CDM Solution.
d. Area D is the Federal CDM Dashboard.

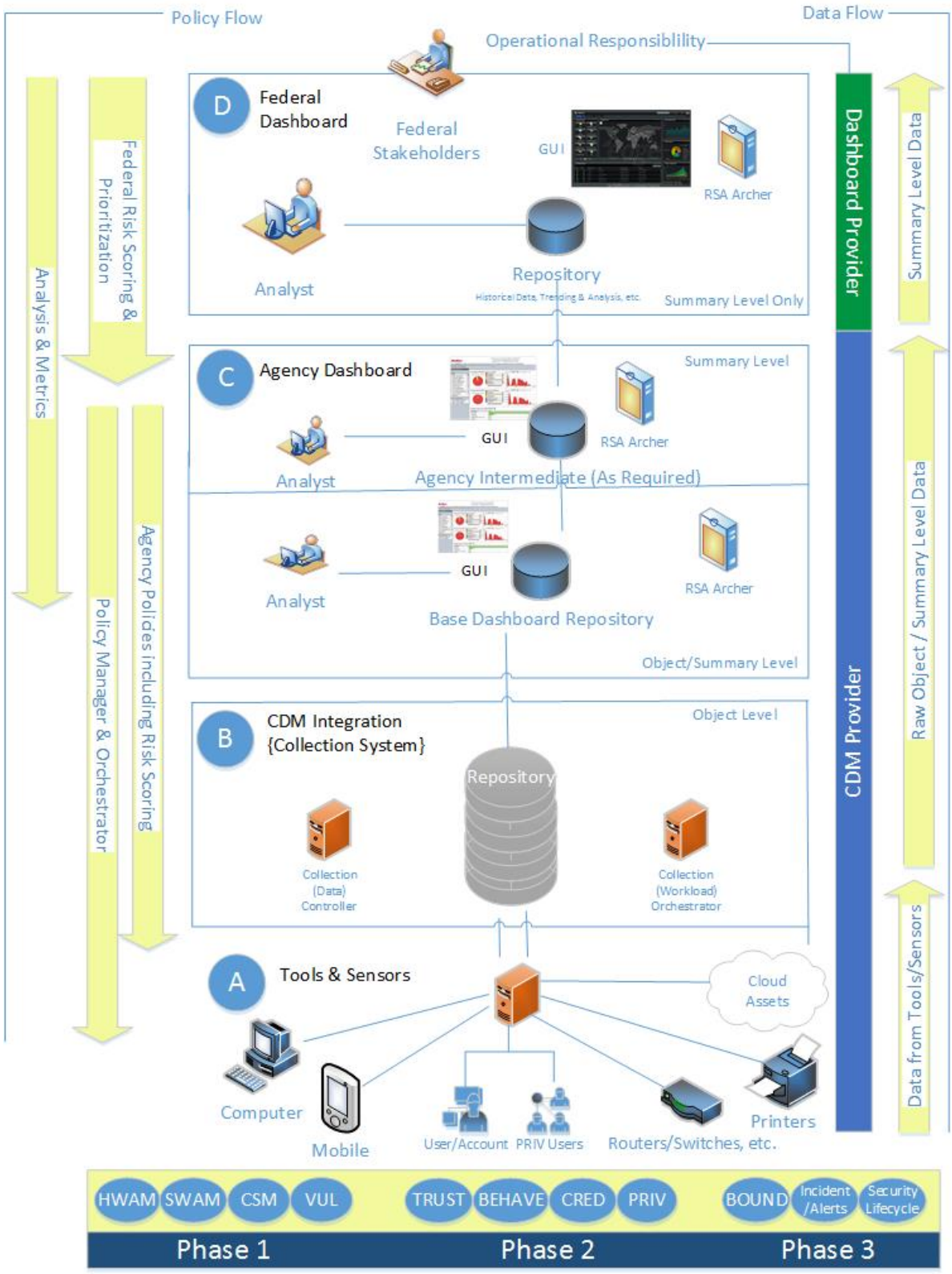

Diagram 2: CDM Architecture

C.4.2 CDM DESIRED FUTURE STATE

The CDM Solution at each Agency shall meet the operational and functional requirements as detailed in CDM Technical Capabilities Requirements Documents, Volumes 1 and 2 (**Section J, Attachments Y.1 and Y.2**) for all CDM areas.

The Government requires an integrated solution that includes support for each Phase of the CDM Program. This multi-phase integrated solution will provide a common set of capabilities across the Agencies to fulfill the capabilities of the four phases of the CDM Program. The Government desires continued enhancement of data aggregation for the Agency Dashboards, then integration through the Federal Dashboard to improve the visibility and identification of cyber threats to Federal Networks. In support of the existing CDM Solution, the contractor shall sustain an integration layer to the Agency and Federal Dashboards, update the Agency Dashboard releases, and integrate the Phase 1 and Phase 2 capabilities. Maintaining the current CDM Solution is not merely continuing a steady state. It requires flexibility, agility, and responsiveness to the evolving cyber threats facing Government networks.

The proposed CDM Solution shall leverage, to the maximum extent possible, modern practices and COTS technology to iteratively develop and deploy an integrated CDM Solution.

The CDM Solution shall be designed and developed, first and foremost, with the Agencies and their end users' experience in mind. The contractor's proposed CDM Solution shall advance the CDM Program's objective to provide a common set of capabilities, but be configured and tailored for DHS needs to provide easy access to the appropriate workflows, tools, reports, and data. The user solutions shall be designed in a way that is easy to use so as to reduce the need for system training.

Given the criticality of the CDM mission, the CDM Solution shall:

a. Meet or exceed industry standards for system availability.
b. Secure certain data in a way that ensures it can be seen and accessed only by those with a "need to know."
c. Integrate seamlessly with all legacy applications and external partners and not cause any disruption to mission essential Agency systems and networks.

The CDM Solution shall allow the data to be aggregated and cleaned to support data analytics and reporting needs without adversely impacting the performance of transactional systems/applications.

Due to rigid governance structures, diversity of mission, and the interconnectedness of the Agencies' environments, most Agencies have yet to develop an enterprise-class IT solution using modern system development practices. Regardless, the CDM Program has a strong preference for utilizing modern development methodologies including, but not limited to, Agile Scrum, Kanban, or Scaled Agile Framework (SAFe).

CDM tools and sensors will need to be refreshed as appropriate. The CDM Solution shall provide continued integration, operation, and maintenance of the Agency level CDM Dashboard ensuring that all installed CDM tools and sensors report to the Agency Dashboard, as necessary. The Government recognizes that many of the CDM tools and sensors are able to meet multiple phase capabilities; therefore, any solution must to the maximum extent possible and practicable

build off of the existing CDM investments. The CDM program requires improved support to identify efficiencies and cost savings, as well as progress tracking and the ability to track deployment schedules across the Agencies.

C.4.3 CDM TECHNICAL CAPABILITIES

The CDM Program is organized by phases, which are not necessarily sequential, and the Government may require the contractor to provide support on multiple phases in parallel. Each CDM phase consists of multiple CDM capabilities, which are summarized in the following sections. The detailed functional and operational requirements of the capability areas can be found in the CDM Technical Capabilities Requirements Document, Volume 2 (**Section J, Attachment Y.2**). The Government desires that the contractor leverage existing Agency investments when developing solutions for CDM capabilities. The contractor shall provide support to the **Section C.6** Tasks to accomplish the following:

C.4.3.1 MANAGE "WHAT IS ON THE NETWORK"

CDM Phase 1 requires the contractor to acquire, deploy, and maintain CDM approved products that support the CDM Program Phase 1 capabilities (i.e., Hardware Asset Management (HWAM), Software Asset Management (SWAM), Configuration Setting Management (CSM), and Vulnerability Management (VUL)).

The focus of CDM Phase 1 is to manage assets by identifying "what is on the network." Specifically, this includes identifying the existence of hardware, software, configuration characteristics, and known security vulnerabilities. HWAM and SWAM cover verification and validation for the existence of hardware devices and the accurate identification of approved software components. CSM covers the verification and validation that hardware devices have the correct security configuration settings, and the system platform is hardened to reduce the platform attack surface. VUL covers verification and validation of preventing and detecting software vulnerabilities to measure software assurance for built and acquired software components.

Each Agency in this TO has made Phase 1 investments, and the contractor shall identify and fill any existing gaps in Phase 1 functionality. This TO expands the CDM Phase 1 functionality to assets that were not previously covered; these are identified in **Table 1: CDM Phase 1 Capabilities**.

Functional Area	Assets Targeted for Coverage by Prior CDM TOs	Additional Assets Targeted for Coverage through this TO
CDM Phase 1		
HWAM	End point (Workstations, Servers) Network Devices (infrastructure) IP addressable assets	Mobile Devices and Mobile Device Manager (MDM) (h) Cloud- Based Assets (g)

Functional Area	Assets Targeted for Coverage by Prior CDM TOs	Additional Assets Targeted for Coverage through this TO
CDM Phase 1		
SWAM	Operating System (a) Common Applications (b) Other Applications (c) Application Integrity (e.g., Whitelisting) (d)	Mobile Devices (h) Cloud- Based Assets (g) Code Validation (e)
CSM	Operating System (a) Common Applications (b)	Mobile Devices (h) Cloud- Based Assets (g) Database (DB)/Web Common Weakness Enumerations (CWEs) (f)
VUL	Operating System (a) Common Applications (b)	Mobile Devices(h) Cloud- Based Assets (g) DB/Web CWEs (f)

Table 1: CDM Phase 1 Capabilities

The following defines the assets identified in **Table 1**:

a. Operating System - As defined in the National Vulnerability Database (NVD) product category of "Operating System" within the Common Platform Enumerations (CPEs).
b. Common Applications - Generally defined in NVD as not "Operating System," to include categories as "desktop application" or "database management" for the CPE.
c. Other Applications - Software that does not have identification within NVD (SWAM).
d. Application Integrity - The part of SWAM that assures the asset identified is a correct and proper instance and is fully authorized. This is usually done through a whitelisting tool and method (SWAM).
e. Code Validation - The part of SWAM that assures the code used to create applications does not contain vulnerabilities.
f. DB/Web CWEs - This is for products specifically designed to manage Database/Web vulnerabilities or configuration settings and reporting in the form of CWEs versus Common Vulnerability Enumerations (CVEs).
g. Cloud Assets - As defined in the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-145, "cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."
h. Mobile Devices and MDM - Mobile device scope will include integration services with existing Agency MDM solutions and the extent to which the MDM is compliant with Agency defined MDM security benchmark. As defined in NIST SP 800-124 Rev 1 (or most current version), "The following hardware and software characteristics collectively

define the baseline of mobile devices:

1. A small form factor
2. At least one wireless network interface for network access (data communications). This interface uses Wi-Fi, cellular networking, or other technologies that connect the mobile device to network infrastructures with connectivity to the Internet or other data networks
3. Local built-in (non-removable) data storage
4. An operating system that is not a full-fledged desktop or laptop operating system
5. Applications available through multiple methods (provided with the mobile device, accessed through web browser, acquired and installed from third parties)"

The expansion of CDM capabilities to Agency Cloud and Mobile environments are addressed in the two following sections.

C.4.3.1.1 COVERAGE OF CLOUD ASSETS

The approach to expanding CDM capabilities to Agency cloud environments requires that the cloud be viewed as two distinct ecosystems. In the first cloud ecosystem, an Agency has identifiable assets that would appear as extensions to the Agency's on premise ecosystem (this could be viewed as a private Infrastructure as a Service (IaaS)). In this scenario, the standard CDM architecture that is used for an on premise CDM Solution shall be extrapolated to cloud assets.

In the second cloud ecosystem, full transparency to assets is not available, such as in a shared service and/or the mechanism used in defining the relationship between the Cloud Service Provider (CSP) and Agency. In this cloud ecosystem only the applicable tracking of CDM metrics applies, which in general is information provided within the Federal Risk and Authorization Management Program (FEDRAMP) process and agreements. Major items (several of which are beyond the Phase 1 requirements) that need to be conveyed to the Agency from the CSP would include:

a. Vulnerabilities of concern to the Agency
b. Incident Response interactions
c. Method of Control Assessment to integrate to Agency's Ongoing Assessment/Authorization
d. Processes/mechanisms for supporting government's post-incident forensics activities
e. Enterprise Account hijacking as it pertains to Agency virtual environment(s)
f. Availability and support of Application Programming Interface (API) for Agencies to automate the extraction of necessary logs that provides situational awareness (e.g., netflow, user access, etc.)
g. Integration of security logs into the Agency security toolsets
h. CSP approach to data deletion
i. CSP Ability to mitigate Distributed Denial of Service (DDOS) attacks
j. Disclosure of malicious provisioning of CSP enterprise resources to Agency customers

The second cloud ecosystem, will require identification of a connection mechanism to the CSP service data source and establish a work flow to provide this information to the Agency's CDM Solution, and ultimately to the CDM Dashboard. The development of this connection mechanism will address all requirements of CDM Technical Capabilities Requirements Document, Volumes 1 and 2 (**Section J, Attachments Y.1 and Y.2**), unless otherwise noted, in which case a rationale for exclusion will be provided. For example, in Phase 1, only VUL requirements may be addressed since HWAM, SWAM, and CM are not under the control of the Agency.

C.4.3.1.2 COVERAGE OF MOBILE ASSETS

The Agencies supported in this TO are expected to establish and deploy an enterprise mobile solution, like an MDM, that will support mobile asset reporting and policy control. Establishing an MDM and providing any related infrastructure are not within the scope of this TO and are planned to be provided by the Agency. Further, configuring an existing Agency MDM according to security benchmarks is not planned to be within the scope of this TO. CDM data will be integrated from existing Agency mobile solutions, such as an MDM, into the Agency's CDM Solution. To accomplish this, both a data exchange mechanism to an Agency deployed MDM (or similar mobile enterprise solution) and a work flow to provide this information to the Agency's CDM Solution, and ultimately to the CDM Agency Dashboard, will be required.

C.4.3.2 MANAGE "WHO IS ON THE NETWORK"

CDM Phase 2 requires the contractor to acquire and deploy CDM approved products that support the CDM Phase 2 capabilities (TRUST, BEHAVE, CRED, and PRIV).

The focus of CDM Phase 2 is to determine "who is on the network." Specifically, this includes identifying and determining the users or systems with access authorization, authenticated permissions and granted resource rights. The CDM Phase 2 capabilities collectively cover the verification and validation of allowed user privileges, user owned credentials, user security behavior training and appropriately granted resource access rights to users.

Each Agency in this TO has made or is in the process of making Phase 2 investments, and the contractor will identify and fill any existing gaps in Phase 2 functionality. This TO expands CDM Phase 2 functionality to assets that were not previously covered, and are identified in **Table 2: CDM Phase 2 Capabilities**.

Functional Area	Assets Targeted for Coverage by Prior CDM TOs	Additional Assets Targeted for Coverage through this TO
CDM Phase 2		
TRUST	Agency Users/Accounts	Accounts for Cloud/Mobile Assets
BEHAVE	Agency Users/Accounts	Accounts for Cloud/Mobile Assets
CRED	Agency Users/Accounts	Accounts for Cloud/Mobile Assets

PRIV	Agency Users/Accounts	Accounts for Cloud/Mobile Assets

Table 2: CDM Phase 2 Capabilities

In **Table 2**, the following definitions apply:

User - A generic term that applies to any entity (including non-person entities) that access any resource, physical or logical, in an organization.

Account - The means by which a user can access a system.

C.4.3.3 MANAGE "WHAT IS HAPPENING ON THE NETWORK AND HOW IS THE NETWORK PROTECTED"

CDM Phase 3 requires the contractor to acquire and deploy CDM approved products that support the CDM Program Phase 3 capability areas of Manage Events (MNGEVT); Operate, Monitor, and Improve (OMI); Design and Build in Security (DBS); and Boundary Protection (BOUND).

MNGEVT is preparing for events/incidents, gathering appropriate data from appropriate sources, and identifying incidents through data analysis. MNGEVT covers verification and validation of processes, policies, and procedures supporting cybersecurity preparation, audit and log data collection, security analysis of audit/log data, and incident reporting to provide forensic evidence of malicious or suspicious behavior (Section J, Attachment Y.2, Section II – 4.2).

OMI includes audit data collection and analysis, incident prioritization and response, and post-incident activities (e.g., information sharing). OMI covers verification and validation of processes/procedures to prioritize incidents and associated response actions, to quickly mitigate the impact of an incident, take appropriate remediation actions to eliminate the impact (restore normal operations) of the same incident, and to support information sharing and collaboration (both internal and external) to minimize or prevent the impact of future incidents (**Section J, Attachment Y.2**, Section II – 4.3).

DBS is preventing exploitable vulnerabilities from being effective in the software/system while in development or deployment. The DBS process is focused on identifying, controlling, and removing weaknesses/vulnerabilities from the software/system. Exploitable vulnerabilities may include software/system design, coding errors, software/system designs that leave a large and complex attack surface that cannot be defended and weaknesses that can only be exploited during system/software execution. DBS covers verification and validation of preventing and detecting software vulnerabilities to measure software assurance for built and acquired software components (**Section J, Attachment Y.2**, Section II – 4.4).

The focus of BOUND is to provide boundary protection for the interior of the network from all interconnections to other external networks. Specifically, it is the determination of the user/system actions and behavior at the network boundaries and within the computing infrastructure. BOUND covers verification and validation of logical and physical network interfaces to reduce intrusive, malicious, and disruptive attacks, cryptographic mechanisms to ensure confidentiality and integrity of data on the network, and methods to identify security incidents (**Section J, Attachment Y.2**, Section II – 4.1).

The following sections (**C.4.3.3.1** through **C.4.3.3.8**) summarize CDM Phase 3 capabilities that represent a new CDM area of capabilities for the Group E Agencies.

C.4.3.3.1 INCIDENT RESPONSE AUTOMATION

Incident response automation is the orchestration that is necessary to support the respond function with automated tools to the maximum extent possible. Orchestration to support the respond function is focused on providing tools and sensors that provide the following functionalities:

a. Incident response event notification
b. Incident handling data collection
c. Incident monitoring
d. Incident reporting
e. Incident response devices

These capabilities are focused on the aspects of the incident handling process, rather than the aspects of reporting the incident response activities. In each of these capabilities, the focus is on being able to collect and correlate data, analyze the data, and provide notifications to the incident response staff. This capability includes the ability to automate the incident response process, where possible, to include the following functionalities:

a. Scanning for recognition of malicious content
b. Automated malware analysis tools
c. Aggregation of threat intelligence data

Incident response automation (including response) will be focused on collating and condensing relevant information for intelligent decision making that ultimately facilitates positive discovery and reporting of incidents, subject to CDM guidance. The contractor shall work with existing security operation center (SOC) assets under this capability area to provide a holistic solution that achieves the results provided in the CDM Technical Capabilities Requirements Documents (**Section J, Attachments Y.1 and Y.2**).

C.4.3.3.2 ONGOING ASSESSMENT

The Government requires a capability to help achieve greater automation, accuracy, and frequency related to the implementation status of Agency NIST 800-53 controls (most current version) and Agency-defined parameters. The current, relatively labor intensive process of conducting NIST 800-53a security assessments offers the CDM Program an opportunity to enable significant efficiencies, cost-savings, and increased data quality by incorporating existing CDM data and technologies with new capabilities.

Ongoing assessment relates the existing Agency Dashboard object and/or summary information to an Agency's associated NIST SP 800-53 controls as defined and implemented so that each Agency's posture is continuously automated for Agency authorization decisions relative to their stated risk tolerance.

The objective of ongoing assessment is the continuous assessment of Agency security and privacy policies related to static object attributes (i.e., actual state and desired state) for threat

behaviors which impact the security and privacy posture of an Agency's existing NIST SP 800-53 controls and countermeasures. Ongoing assessment also encompasses the identification of new component weaknesses and vulnerabilities that represent unauthorized deviations to an Agency.

C.4.3.3.3 ONGOING AUTHORIZATION

The Government has a need to improve the efficiency, data quality and currency, and reduce cost related to current security authorization processes.

Ongoing authorization uses the results of the ongoing assessment of NIST SP 800-53 controls for all previous phases of CDM as a set of inputs for the orchestration of ongoing authorization, risk assessment, and acceptance processes. These processes support and orchestrate with the needs of Agency personnel assigned to oversee Agency risk-tolerance in accordance with the status of the required NIST 800-53r4 controls and Agency-specific parameters.

Ongoing authorization allows Agencies, senior risk management, and cybersecurity personnel the ability to quickly assess security risk against acceptable security risk levels and adjust security requirements or NIST SP 800-53 controls and countermeasures to ensure that an acceptable level of security risk is maintained. This approach is much more efficient than the traditional multiyear security assessment and authorization methods with which Agencies maintain and accept residual risk.

Ongoing Authorization provides the ability to automate the determination and necessary updates to NIST 800-53 controls and countermeasures, to allow systems to be evaluated and authorized when CDM system changes are made, or automate Plan of Action and Milestone (POA&M) creation when security controls are identified as not maintaining risk at approved levels as defined by Agencies.

C.4.3.3.4 BOUND FILTERING BY NETWORK

The BOUND function provides Agencies with visibility into the risk associated with connections or access to networks, systems, and data. To provide this visibility, BOUND Filtering by Network (also referred to as Manage Network Filters and Boundary Controls (BOUND-F)) utilizes filters that include devices like firewalls and gateways that sit at the boundary between enclaves, such as a trusted internal network or subnet and an external or internal, less-trusted network. The Government considers an enclave as a collection of information systems connected by one or more internal networks under the control of a single authority and security policy, with the systems being structured by physical proximity or by function, independent of location.

The filters apply sets of rules and heuristics to regulate the flow of traffic between the trusted and less trusted sides based on network attributes (such as ports and protocols). The overall objective of BOUND-F is to reduce the probability that unauthorized traffic passes through a network boundary.

This BOUND-F functionality provides an analysis of an Agency's existing network-based filtering capabilities and improves and augments this protection for an Agency. Additionally, it includes the ability to examine encrypted content if possible. The types of network devices/capabilities that are encompassed by BOUND-F include, but are not limited to:

a. Packet filtering
b. Proxies
c. Network access protection
d. Encapsulation Filtering

   Also included would be:

   1. Internet for Federal Government:
      i. EINSTEIN
      ii. Trusted Internet Connection (TIC)

BOUND-F requires that boundary policies include monitoring, reviewing, and reauthorizing consistent with any Agency policy. In addition, BOUND-F allows for the reporting of the effectiveness of the detect/protect characteristics of these technical elements as well as relevant asset information are also required.

C.4.3.3.5 BOUND FILTERING BY CONTENT

Content based perimeter protection prevents unwanted content from entering or leaving the gateway of a network. BOUND-F content filtering examines network traffic at the application level to block or filter malware or prohibited traffic from entering or leaving the network. The two common areas of content filtering are web (HTTP) and email (SMTP). Web content filter includes protecting servers from common web attacks by using a Web Application Firewall (WAF) to inspect HTTP traffic. Web Malware protection is used to inspect web traffic for malicious code and block it before it can reach endpoints in the Agency network. Web content filters block Agency endpoints from reaching prohibited websites and Internet Protocol (IP) addresses. Email content filtering uses message content such as attachments, headers, or content in the message body, to block an email based on Agency policies. Email content filtering can also provide anti-phishing capabilities. Email malware protection inspects and analyzes email traffic for malicious content and blocks or prevents its spread.

BOUND-F filtering by content provides an analysis of an Agency's existing web and email content filtering capabilities and improve and fill in content filtering protection for an Agency. Capabilities include the ability to examine encrypted content where appropriate. In addition, BOUND-F filtering by content allows for the reporting of the effectiveness of the detect/protect characteristics of these technical elements as well as relevant asset information.

C.4.3.3.6 DATA-BASED PERIMETER PROTECTION

The DBS function of data-based perimeter protection focuses on the identification and prevention of data exfiltration within the Agency. Data-based perimeter protection is a broad category of protections that includes the technologies used for Data Leak/Loss Prevention (DLP). This protection provides the capability to mitigate the effects of insider threat activities to include, but are not limited to the following:

a. Manipulating files without authorization
b. Printing protected data
c. Exporting protected data outside of the Agency

d. Intercepting protected data as it transits to the Agency network

The technologies to implement this type of protection typically focus on the inspection of packets as they move across the network with the objective of identifying potential data movement attempts. These technologies can also include the use of device-based diagnostics to recognize unusual activities involving the protected data. This protection can be in the form of blocking, monitoring, or notification when a suspected data loss event is in progress.

C.4.3.3.7 BOUND-ENCRYPTION

Cryptographic mechanisms protect credentials, data at rest, and data in motion. An identity credential is a digital representation of a user. The identity credentials are often implemented on an integrated circuit smart card, in particular the Federal Personal Identity Verification (PIV) card as specified in Federal Information Processing Standards (FIPS) -201-2. FIPS 201 credentials commonly include information such as private keys, pins, digital certificates, and encoded biometric values. Credentials are used to authenticate users, systems, software packages and other resources in the system. Data at rest protection includes encryption of individual files, as well as encryption of entire volumes/disks. Components of data at rest encryption include both the encryption software itself and the encrypted data. Data in motion cryptography involves the use of application security protocols such as Secure/Multipurpose Internet Mail Extensions (S/MIME) and Secure Shell (SSH); web-based transactions using Secure Sockets Layer (SSL) / Transport Layer Security (TLS); and Virtual Private Networks (VPNs) using Internet Protocol Security (IPsec) and SSL/TLS.

Together these cryptographic techniques and related cryptographic keys/credentials provide critical security functions to support the confidentiality, integrity and authenticity of network functions both internally to protect insider threats and externally to prevent malicious behaviors.

Boundary Encryption (BOUND-E) functionality provides indications of improper cryptographic behavior and/or hardware/software misconfiguration on Agency Assets. Cryptography must be properly implemented and configured in order to provide the desired level of protection. Support of BOUND-E provides Agencies with capabilities to collect policies from hardware device, software product, and cryptographic implementation configuration settings, to ensure that the right implementations are being used and configured properly. In addition, support of BOUND-E provides capabilities to manage and monitor cryptographic key management systems.

Targeted Capabilities include, but are not limited to the following:

a. Ability to monitor public key Certificate Authority compliance with the Federal Root Certificate Policy Authority.
b. Ability to monitor PIV card compliance with FIPS 201-2 Key Management and Cardholder Authentication requirements.
c. Ability to collect as-is state data elements and attributes and compare with desired state attributes per the CDM Technical Capabilities Requirements Document, Volumes 1 and 2 (**Section J, Attachments Y.1 and Y.2**).

C.4.3.3.8 INCORPORATION OF SYSTEM ASSURANCE (SOFTWARE/HARDWARE)

Improving Agency capabilities with respect to secure systems engineering development is well understood to be a best practice and one that readily reduces cost and risk to IT projects. This is the implementation of the requirements identified as the design/build-in security capability. Supporting system assurance reduces the attack surface for network and infrastructure components during acquisition, development, and deployment and reduces project costs associated with poor security engineering practices.

The following DBS capabilities support this goal:

a. Supply Chain Risk Management (SCRM) attributes
b. Software development assurance (code inspection/analysis)
c. Application weakness detection (web-based vulnerabilities such as CWE and secure configuration, as well as database focused)

Supply Chain Risk Management (SCRM)

The purpose of SCRM is to enable the provisioning of the least vulnerable solutions to agencies, through a robust assessment of supply chain risks, communication of those risks to the Agencies, and the appropriate response and monitoring of those risks throughout the entire system life. SCRM impacts this TO in two distinct ways. First, the contractor shall apply best SCRM practices (to include any teaming partners or vendors) within the execution of the TO. The second SCRM impact is through the contractor assisting Agencies to establish continuous improvement (to include measurable outcomes) within the Group E Agencies in terms of Agency-specific governance.

Software Development Assurance (code inspection/analysis)

Software Development Assurance introduces the ability to develop secure code via code inspection and to use security testing and evaluation during development, such as those prescribed by the NIST 800-53r4 control, SA-11 Developer Security Testing and Evaluation. Software Development Assurance also assists Agencies in ensuring that security controls are implemented correctly, operating as intended, enforcing the desired security policy, and meeting established security requirements as modeled after production configurations. Security testing and evaluation includes flaw remediation/correction processes, static code analysis, other types of analysis and reviews, and testing artifacts.

Software development assurance also includes increasing scope of existing CDM tools from Phase 1 into development enclaves and network boundaries, such that production machine-level desired states are integrated into development efforts to ensure continuity of configurations.

Application weakness detection

During deployment and operation, runtime software systems continuously assess and monitor for vulnerabilities and exploits of software weaknesses, in designated Agency networks, to the maximum extent possible. Dynamic assessment tools are utilized to support general software assurance needs in both development and production scenarios, where possible, and tailored to address availability and performance concerns.

In addition, the operating system platform shall be monitored for malicious attacks on the weaknesses and vulnerabilities of the operating system, platform tools, and utilities.

C.4.3.4 MANAGE "HOW DATA IS PROTECTED ON THE NETWORK"

CDM Phase 4 capabilities described below support the overall CDM Program goals to identify cybersecurity risks on an ongoing basis, prioritize these risks based upon potential impacts, and enable cybersecurity personnel to mitigate the most significant problems first. These fundamental requirements may be accomplished in new and innovative methods that transcend the current CDM architecture model. The following sections are examples of portions of the solutions that could be associated with protecting data on the Agencies' networks.

C.4.3.4.1 MICRO-SEGMENTATION

Micro-segmentation is the virtualization of the data center or a cloud computing structure. It is a security technique that integrates security directly into the virtualized workload and eliminates the requirement of hardware-based firewalls. One of the characteristics of micro-segmentation is that it is persistent. With micro-segmentation, security policies can be placed on the virtual connections that can move with an application if the network is reconfigured. This makes security on the network persistent as well as ubiquitous. Hence, micro-segmentation enhances the current and future security posture of a network. It is assumed that measure micro-segmentation will be at par with those of conventional segmentation, such as system asset inventory and the items found in BOUND.

C.4.3.4.2 DIGITAL RIGHTS MANAGEMENT (DRM)

Since there are limitations to the tools and methods used to support data-based perimeter protection due to inherent limitation of control mechanisms, DRM provides an alternative method for enforcement of these data-based controls. Enterprise DRM, also commonly referred to as information rights management, provides persistent protection of information regardless of its transience within or external to the enterprise. The DRM tool can be facilitated by a combination of onsite or offsite technology presence (e.g., cloud provided) and should provide sufficient protection mechanisms such that unauthorized access to the data is prevented through strong technical means (e.g., encryption of data) which is capable of being centrally managed by the enterprise. DRM tools should provide some level of assurance that loss of the digital artifacts to an untrusted agent do not necessarily result in the loss of the data contained within. The CDM Program intends to provide supplemental requirements and guidance in forthcoming documentation to clarify the specific mission needs that are necessary under the digital rights management functional area.

C.4.3.4.3 ADVANCED DATA PROTECTIONS

As with DRM, there are limitations to the tools and methods used to support data-based perimeter protection. There are inherent limitations of control mechanisms, advanced data protection safeguards, and the protection of important information from corruption, loss, or exposure to unintended recipients. The term advanced data protection is used to describe both operational considerations such as backup of data and disaster recovery/business continuity, as well as information security considerations such as data classification, access controls, data

transformation, and monitoring and auditing. Two functionalities associated with advanced data protection, specifically Data Lifecycle Management (DLM) and Information Lifecycle Management (ILM), are addressed below.

DLM is the automated movement of critical data to online and offline storage and the protections applied to maintain confidentiality, integrity and availability of that information in the various locations for the specified purpose. Capabilities associated with DLM include but are not limited to:

a. Encryption and key management
b. Data masking
c. Backup and recovery of data
d. Remote data storage to facilitate disaster recovery
e. Storage system security

ILM is the strategy for understanding the value of information and protecting important information assets. Similar to DLM, it operates on the value of data, taking the context of the information into consideration. An example of the difference between DLM and ILM is the information that comprises Personal Identifiable Information (PII) and Sensitive Personal Identifiable Information (SPII). PII is any information that permits the identity of an individual to be directly or indirectly inferred, including any information that is linked or linkable to that individual. SPII is PII, which if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. Some categories of PII are sensitive as stand-alone data elements such as Social Security Number (SSN), driver's license number, passport number, biometric identifiers, etc. Other information such as citizenship, medical information, date of birth, or account passwords is sensitive when associated with the identity of an individual. Capabilities associated with ILM include, but are not limited to:

a. Discovery and classification of data
b. Data vaulting
c. Data labeling
d. Data masking and sub-setting
e. Data access firewall
f. Data access monitoring
g. Normalized repository of auditing data

C.4.4 IT DELIVERY MODELS

The CDM Solution must recognize and incorporate the IT delivery models in place at the Group E Agencies. The following discussion describes models that may be implemented at the Group E Agencies.

Information on whether each Agency uses the centralized or federated model will be noted in the Government-provided Agency-specific IT/Network Environment Summary Information available in the eRR.

a. Centralized Model. In the centralized model, top-down responsibility for IT acquisition, solutions delivery, conceptualizing, developing, and implementing IT solutions for all parts of the business is controlled by the Agency in one place. This is usually a Headquarters (HQ) function, but may also be delegated to one of the Agency's larger components.

b. Federated Model. In the federated model, the Agency HQ IT unit (usually the Chief Information Officer/Chief Information Security Officer's (CIO/CISO's) office) may have primary responsibility for architecture, common infrastructure and services, and standards decisions, while each Agency IT department has primary responsibility for application resource decisions. Agency IT managers report to the Agency Director as well as the central IT organization. In a few Agencies, the federated model is highly decentralized, with the solutions delivery aligned with the Agency component and IT managers reporting to the Agency component Director. When coordination happens, it is achieved in IT management and executive councils.

C.5 REQUEST FOR SERVICE (RFS)

The Government requires a flexible approach to support the evolving CDM technical capabilities in a rapidly changing cybersecurity environment during the entire life of the TO. To address the evolving needs of the supported Agencies, the Government will execute an RFS process that will further define Agency-specific requirements for initial delivery and/or additional support of a CDM capability or service.

The RFS will state the purpose, supported Agency(ies), primary place of performance, anticipated tasks/subtasks required, technical details of the requirement (including references to the CDM Technical Capabilities Requirements Documents, Volume 1 and Volume 2 (**Section J, Attachments Y.1 and Y.2**) when appropriate), other supporting details related to the requirements (e.g., security requirements, expected execution timelines, Government-Furnished Information (GFI), and tailored System Engineering Lifecycle (SELC) requirements), and expected timeline for return of the RFS Response. Each RFS will apply performance-based outcomes and standards as appropriate to the requirement. High quality products and services delivered in a timely and cost-effective manner will be the primary criteria for the work performed under an RFS.

After receiving an RFS, the contractor shall develop and deliver an RFS Response in accordance with **Section C.6.1.12 (Subtask 1.12)**. The contractor shall only execute actions identified in the RFS Response after the Government provides written approval. All cost and schedule measures associated with the execution of a specific RFS shall be clearly identified in the Integrated Master Schedule (IMS), cost reports, and invoices.

The RFS Tracking Table (**Section J, Attachment AI**) identifies RFS actions approved for execution during the TO.

C.6 TASKS

Task 1: Provide Project Management

Task 2: CDM Solution and Dashboard Support

Task 3: Integrate New CDM Capabilities

Task 4: Expanded Agency Services

Task 5: Surge Cybersecurity Critical Incident Support

C.6.1 TASK 1 – PROVIDE PROJECT MANAGEMENT

The contractor shall provide project management support under this TO. This includes the management and oversight of all activities performed by contractor personnel, including subcontractors, to satisfy the requirements identified in this Performance Work Statement (PWS). The contractor shall identify a Project Manager (PM) by name that shall provide management, direction, administration, quality assurance, and leadership of the execution of this TO.

The contractor shall use industry-best standards and proven methodologies that ensure all TO activities are identified, documented, and tracked so that the TO can continuously be evaluated and monitored for timely and quality service. The contractor shall notify the Federal Systems Integration and Management Center (FEDSIM) Contracting Officer (CO) and Contracting Officer's Representative (COR) and the DHS Technical Point of Contact (TPOC) of any technical, financial, personnel, Organizational Conflict of Interest (OCI), or general managerial problems encountered throughout the life of the TO.

C.6.1.1 SUBTASK 1.1 – COORDINATE A PROJECT KICK-OFF MEETING

The contractor shall coordinate with the FEDSIM CO to schedule, coordinate, and host a Project Kick-Off Meeting at a location approved by the Government (**Section F, Deliverable 03**). The meeting will provide an introduction between the contractor personnel and Government personnel who will be involved with the TO. The meeting will provide the opportunity to discuss technical, management, and security issues and travel/product authorization and reporting procedures. At a minimum, the attendees shall include contractor Key Personnel; representatives from DHS, including the DHS TPOC; the FEDSIM CO; the FEDSIM COR; and Government representatives from each Agency supported by this TO.

At least three days prior to the Kick-Off Meeting, the contractor shall provide a Kick-Off Meeting Agenda (**Section F, Deliverable 02**) for review and approval by the FEDSIM COR and DHS TPOC prior to finalizing. The agenda shall include, at a minimum, the following topics/deliverables:

a. Introduction of team members and personnel:
    1. Roles and responsibilities, including staffing plan and project organization
    2. Overview of the contractor's organizational strategy to support varying locations of work and multiple Agencies
b. Communication Plan/Lines of communication overview (between both the contractor and Government)
c. Updated Draft Transition-In Plan (**Section F, Deliverable 23**) and discussion
d. TO Management:
    1. Overview of the TO technical approach, including RFS-DHS-0003

2. Overview/outline of the draft Project Management Plan (PMP) (**Section F, Deliverable 17**)
3. Overview of project tasks, schedule, and establishment of performance metrics
4. Identified risks and issues and applicable mitigation plans
5. Overview of the draft IMS (**Section F, Deliverable 20**) (shows major task, milestones, and deliverables; planned and actual start and completion dates for each)
6. Overview of SELC process
7. Overview of the TO draft Quality Control Plan (QCP) (**Section F, Deliverable 05**)
8. TO logistics

e. TO Administration:

1. Review of GFI and Government-Furnished Property (GFP)
2. Deliverable process and procedures
3. Review of Financial Status Reporting format: including DHS reporting, Agency reporting, invoice review and submission procedures (**Section G.2**), and tracking of funds by Client Tracking Number (CTN) and cost savings
4. Invoice Requirements
5. Travel notification, process, and reporting
6. Request to Initiate Purchase (RIP) submission review and approval process
7. Security requirements/issues/facility/network access procedures
8. Sensitivity and protection of information
9. Reporting requirements, (e.g., Monthly Status Report (MSR))
10. Proposed reports of technical metrics on operation of the CDM Solution as defined in the PMP, to include percentage of tools deployed to applicable assets relative to adjudicated asset scope with the Agency
11. Review of RFS process (**Section C.5**)
12. Review of Draft Master Repository (**Section C.6.1.2, Section F, Deliverable 14**)
13. Review of Procurement Report format
14. Review of Problem Notification Report (PNR) process (**Section J, Attachment Q**)
15. Additional administrative items including press releases

The Government will provide the contractor with the number of Government participants for the Kick-Off Meeting and the contractor shall provide sufficient copies of the presentation for all present.

The contractor shall draft and provide a Kick-Off Meeting Report (**Section F, Deliverable 11**) documenting the Kick-Off Meeting discussion and capturing any action items.

C.6.1.2 SUBTASK 1.2 – MAINTAIN A MASTER REPOSITORY

The contractor shall develop and maintain a Master Repository (**Section F, Deliverables 14, 15, and 16**) of all submitted RFSs, Travel Authorization Requests (TARs), RIPs, and deliverables. At a minimum, this repository shall include dates submitted and approved by the Government,

financial information (i.e., estimated costs and costs invoiced) if applicable, pending Government actions, and any other pertinent information associated with the repository items identified above. The master repository is evolutionary and shall be continuously updated as requests/deliverables are submitted/responded to by the Government.

The contractor shall present a master repository format at the Kick-Off Meeting for Government review. The Government will provide written approval of the proposed format via the FEDSIM COR and this approved format shall be utilized over the life of the TO. The Government may request updates to the format based on CDM PMO repository requirements and Agency needs. Any changes to the format will be requested in writing via the FEDSIM COR. The contractor shall deliver all contents of the repository on a quarterly basis and upon Government request.

C.6.1.3 SUBTASK 1.3 – PROVIDE MONTHLY STATUS REPORT (MSR) AND CONVENE MONTHLY STATUS BRIEFING

The contractor shall develop and provide an MSR (**Section F, Deliverable 08**) via email to the DHS TPOC and the FEDSIM COR. The MSR shall briefly summarize, by task area, the TO management and technical progress to date, as well as provide the current information indicated below. The purpose of this report is to ensure all stakeholders are informed of key elements of the CDM project at the Agency-level, provide opportunities to allow stakeholder input, and coordinate resolution of risks and issues and change management as required. The MSR shall be prepared in accordance with the Monthly Status Report Template (**Section J, Attachment H**).

The contractor shall conduct a Monthly Status Briefing (**Section F, Deliverable 09**) to brief the FEDSIM COR, DHS TPOC, Agency representatives, and other Government stakeholders on the status of the TO and activities. The Government reserves the right to change this requirement to in-person monthly status meetings as required. The purpose of this meeting is to ensure all stakeholders are informed of the monthly activities and the MSR, provide opportunities to identify other activities and establish priorities, and coordinate resolution of identified problems or opportunities. The contractor PM shall provide minutes of this meeting in a Meeting Report, including attendance, issues discussed, decisions made, and action items assigned (**Section F, Deliverable 11**).

The Monthly Status Briefing shall include, at a minimum:

a. The status of activities during the reported period, by task area
b. Project schedule
c. Financial status overview
d. Procurement status of tools/ODCs
e. Status of action items, risks, and issues
f. Progress to date on all items identified in the list above for the MSR

C.6.1.4 SUBTASK 1.4 – CONDUCT QUARTERLY IN-PROGRESS REVIEW (IPR) MEETINGS

The contractor shall conduct a formal IPR (**Section F, Deliverable 10**) at a location approved by the Government. The IPR shall provide a forum for Government review of progress, planning, and issues related to TO performance. The contractor shall utilize the PMP in its discussion of

TO performance. The IPR shall replace the Monthly Status Briefing Meeting for that month. IPRs shall, at a minimum, include:

a. Program status overview
b. Status of CDM Solution, including Dashboard, at each Agency
c. Schedule by task
d. Previous month and quarter activities by task
e. Planned activities for next month and quarter by task
f. Financial status, to include quarterly cost savings report on material and equipment purchases
g. Staffing status by Agency
h. Status of Risks and Issues
i. Actions required by the Government

The contractor shall prepare the IPR agenda, Meeting Report (**Section F, Deliverable 11**), and presentation material. IPRs shall be conducted no less than quarterly; however, more frequent IPRs may be required. The IPR is historically attended by an average of seven to 15 total stakeholders, to include contractor personnel, FEDSIM COR, DHS TPOC, Agency representatives, and other key Government stakeholders.

The fourth quarter IPR meeting of each TO year shall act as an overview of the entire TO year and act as a closeout for the ending TO year. The fourth quarter IPR shall include the above IPR requirements, financial reporting information for the year, Master Repository and Procurement Report information for the years, and planned actions required by the contractor and Government.

C.6.1.5 SUBTASK 1.5 – PROVIDE FINANCIAL REPORTING

This TO will receive funds through different funding streams from DHS and each of the Agencies and will require distinct financial tracking throughout the life of the TO. The contractor shall provide a Financial Report of cumulative expenditures monthly (**Section F, Deliverable 13**) to the FEDSIM COR and DHS TPOC that tracks these distinct separate funding streams. The Financial Report shall include as a minimum:

a. Identification of the funding source.
b. Monthly expenditures by CDM Phase, CTN, and TO level from the start of the POP.
c. Project monthly expenditures and labor hours by CTN and TO level starting with the current month through the end of the POP.
d. Funded levels by TO and by Agency.
e. Labor hours incurred to date by TO and by Agency.
f. Funds remaining by RFS and CLIN.
g. Diagram reflecting funding and burn rate by month for the TO and at the Agency-level.
h. Cumulative invoiced amounts for each CLIN up to the previous month.
i. Actual current and cumulative dollars expensed for small businesses compared to TO subcontracting goals.

The contractor shall present a Financial Report format at the Project Kick-Off Meeting (**Section C.6.1.1**) for Government review. The Government will provide written approval of the proposed format via the FEDSIM CO or FEDSIM COR, and this approved format shall be utilized for the monthly financial reporting requirement. The Government may request updates to the format based on DHS CDM PMO requirements and Agency needs. Any changes to the format will be requested in writing via the FEDSIM CO or FEDSIM COR.

C.6.1.6 SUBTASK 1.6 - PROCUREMENT REPORT

The contractor shall procure the necessary CDM tools and sensors and any ODCs.

The contractor shall develop a Procurement Report (**Section F, Deliverable 52**) in accordance with Procurement Report Template (**Section J, Attachment J**) for the CDM tools and ODCs that are required to support the CDM Solution or any new CDM capabilities over the POP of the TO. The Procurement Report shall initially capture the planned procurement of any CDM tools and sensors, and later be updated to capture the lifecycle of Delivery and Acceptance for the CDM tools and sensors. The Procurement Report shall be a living document and is anticipated to be updated periodically throughout the TO and, at a minimum, for the following instances:

a. RIP and/or RFS Reference Number, as applicable.
b. Proposed cost from RIP, actual cost of products purchased; CDM tools Special Item Number (SIN) price comparison, if available.
c. Cost savings to the Government (i.e., discounts).
d. Product dates of order, delivery, receipt of goods by Agency customer, and implementation.
e. For products that require renewal, the date of expiration.
f. Execution of **Subtask 3.1** – CDM Technical Planning.
g. Identify changes in a planned procurement of CDM tools or ODCs.

The contractor shall work collaboratively with the DHS CDM PMO and Agencies to manage property accountability, to include the transfer of licenses.

C.6.1.7 SUBTASK 1.7 – PREPARE MEETING AND TRAVEL REPORTS

The contractor shall conduct, attend, and participate in various project- and program-related meetings. These meetings may include, but are not limited to, Integrated Project Team (IPT) brainstorming sessions, program management reviews, technical status reviews, document reviews, and contract status reviews.

a. The contractor shall submit Meeting Reports (**Section F, Deliverable 11**) as requested by the FEDSIM COR and/or DHS TPOC to document results of meetings. The Meeting Reports shall include the following information:
    1. Meeting attendees and their contact information, at a minimum, identify organizations represented
    2. Meeting dates
    3. Meeting location
    4. Meeting agenda

5. Purpose of meeting
6. Summary of events (issues discussed, decisions made, and action items assigned)

b. The contractor shall submit a Trip Report (**Section F, Deliverable 12; Section J, Attachment P**), as requested by the DHS TPOC and/or FEDSIM COR. The need for a trip report will be identified when the TAR is submitted.

The Trip Report shall include the following information:

1. Personnel traveled
2. Dates of travel
3. Destination(s)
4. Purpose of trip
5. Summarized cost of the trip
6. Approval authority
7. Summary of events, action items, and deliverables

C.6.1.8 SUBTASK 1.8 – PREPARE A PMP, IMS, AND QCP

Based on the contractor's proposal in response to the solicitation, the contractor shall prepare and deliver a Draft and Final PMP (**Section F, Deliverables 17 and 18**). The PMP shall address work at the first (parent) and second (Component, etc.) levels of the Agency, as appropriate.

The PMP shall contain, at a minimum, the following:

a. Management approach:
    1. Communications and stakeholder management (to include the contractor's organizational chart)
    2. Scope management (to include milestones, tasks, and subtasks required in this TO)
    3. Requirements management
    4. Quality management
    5. Staffing management (to include the Project Staffing Plan)
    6. Procurement management
    7. Logistics management
    8. RFS Management
    9. Cost Management

b. Technical approach:
    1. Work Breakdown Structure (WBS) and WBS dictionary. Include associated responsibilities and partnerships between Government organizations. The WBS should plan for control accounts that allow for tasks to be planned, budgeted, forecasted, and cost collected at a level which allows for summary level organized by Agency.
    2. Risk management, including identified risks, issues, and planned mitigation.
    3. Testing.

c. Training approach

Defect metrics, including but not limited to, reflecting where proposed tools negatively impact Agency assets such as extreme performance latency, or where CDM technical requirements are not satisfied due to error conditions, are required.

The PMP is an evolutionary document that shall be updated annually at a minimum (**Section F, Deliverable 19**). The contractor shall work from the latest Government-approved version of the PMP.

The contractor shall prepare and deliver a Draft and Final IMS (**Section F, Deliverables 20 and 21**) and a Draft and Final QCP (**Section F, Deliverables 05 and 06**) to accompany the PMP as separate deliverables.

The IMS is also an evolutionary document that shall be updated with technical inputs and significant changes as required (**Section F, Deliverable 22**). The contractor shall reflect the Government's requirements in planning for all activities in Tasks 2 through 5 and the tailored DHS or Agency-specific SELC process reviews in the IMS. This includes the Government's requirements that the CDM Solution for each Agency shall be operational as soon as the contractor is able to complete installation, configuration, and required security authorization at individual Agencies. The contractor shall work from the latest Government-approved version of the IMS.

The QCP shall include, but is not limited to, the following:

a. Performance monitoring methods
b. Performance measures
c. Approach to ensure that cost, performance, and schedule comply with task planning
d. Methodology for continuous improvement of processes and procedures, including the identification of service metrics that can be tracked in the TO
e. Government roles
f. Contractor roles

Significant changes represent any alteration, modification, or adjustment to the CDM Solution, cost, or schedule that is sufficiently great or important and worthy of attention in the PMP or IMS. As RFS actions are activated, the IMS shall be updated and resubmitted.

The QCP is also an evolutionary document that shall be updated annually at a minimum (**Section F, Deliverable 07**). The contractor shall work from the latest Government-approved version of the QCP.

C.6.1.9 SUBTASK 1.9 – TRANSITION-IN

The Transition-In Plan shall address the Tasks in **Section C.6**, identifying the roles and responsibilities of the contractor and incumbent, information expected from the incumbent, a draft schedule(s), to include the anticipated timeline for appropriate personnel security processing, and milestones to ensure no disruption of service.

The contractor shall ensure that there will be minimum service disruption to vital Government business and no service degradation during and after the Transition-In period. Each Agency is at

a different stage in its implementation of the CDM Solution; therefore, the Transition-In Plan shall account for the differences in Agency implementation and IT environment. The contractor shall begin Transition-In activities when the Government has accepted the final Transition-In Plan (**Section F, Deliverable 23**). The Transition-In Plan will take into account the current CDM Solution, which includes Phase 1 and Phase 2 investments. CDM Solution support is currently being provided under TO2E which expires on September 10, 2018. The contractor shall update the proposed Draft Transition-In Plan (**Section F, Deliverable 23**) submitted with its proposal, as appropriate, and provide a Final Transition-In Plan (**Section F, Deliverable 24**) within ten business days after receipt of Government comments.

C.6.1.10 SUBTASK 1.10 - TRANSITION-OUT

The contractor shall provide Transition-Out support when required by the Government. The contractor shall facilitate the accomplishment of a seamless transition from the incumbent to an incoming contractor/Government personnel at the expiration of the TO. The contractor shall provide a Draft Transition-Out Plan (**Section F, Deliverable 25**) NLT 150 calendar days prior to expiration of to the base and each option period and the contractor shall provide a Final Transition-Out Plan (**Section F, Deliverable 26**) NLT 120 calendar days prior to expiration of the TO. The Transition-Out Plan shall be organized by Agency. The Government will work with the contractor to finalize the Transition-Out Plan. The contractor shall identify in the Transition-Out Plan how it will coordinate with the incoming contractor and/or Government personnel to transfer knowledge regarding the following:

a. Project management processes
b. Points of Contact (POCs)
c. Location of technical and project management documentation
d. Status of ongoing technical initiatives
e. Appropriate contractor to contractor coordination to ensure a low risk transition
f. Transition of Key Personnel
g. Schedules and milestones
h. Configuration settings of COTS tools
i. Asset management, including license expiration dates, where applicable
j. Actions required of the Government

The contractor shall also establish and maintain effective communication with the incoming contractor/Government personnel for the period of the transition via weekly status meetings or as often as necessary to ensure a seamless transition out.

The contractor shall update the Transition-Out Plan (**Section F, Deliverable 27**) annually and quarterly during the final option period. The contractor shall implement its Transition-Out Plan in accordance with the Government-approved Transition-Out Plan and NLT 90 calendar days prior to expiration of the TO. All facilities, equipment, and material utilized by the contractor personnel during performance of the TO shall remain accessible to the contractor personnel during the Transition-Out period pursuant to the applicable security in-processing and out-processing guidelines.

C.6.1.11 SUBTASK 1.11 – COORDINATE AND COMPLETE SELC REVIEWS

The contractor shall coordinate and complete each SELC review detailed in the DHS SELC Process Overview (**Section J, Attachment X**) for each Agency's CDM Solution. Depending on the contractor's implementation schedule, these SELC reviews shall be completed concurrently or separately by the Agency. Agency specific SELC processes may also be required for Agency sponsored activities and will be stated in the Agency RFS if needed. Deliverables associated with the SELC gate reviews are defined in **Section J, Attachment X**.

C.6.1.12 SUBTASK 1.12 – DEVELOP REQUEST FOR SERVICE (RFS) RESPONSES

The contractor shall develop and deliver an RFS Response (**Section F, Deliverable 28**) for any Government provided RFS. The RFS process is described in **Section C.5**. The contractor developed RFS response shall include a brief overview of the requested services, including any technical relevant details pertinent to the proper execution of the support. In addition, the RFS response shall include a Rough Order of Magnitude (ROM) cost estimate that depicts labor categories and hours by task/subtask, a draft RIP for any CDM tools or supporting ancillary products (i.e., hardware/software) as required , and anticipated travel to meet the requirement.

C.6.2 TASK 2 – CDM SOLUTION AND DASHBOARD SUPPORT

The contractor shall provide CDM Solution and CDM Agency Dashboard support entailing necessary testing and security accreditation support to maintain authorization and providing Tier III support to the CDM Solution. This task also entails updating the CDM Agency Dashboard with each new release of the CDM Agency Dashboard, providing Tier II level support to the CDM Agency Dashboard, and establishing and maintaining operational CDM data feeds from the integration layer to the CDM Agency Dashboard and from the CDM Agency Dashboard to the CDM Federal Dashboard. Both the CDM Agency and CDM Federal Dashboards are developed by the CDM Dashboard provider through another CDM TO. This CDM Dashboard provider will provide releases of the CDM Agency Dashboard and Tier III support for the CDM Agency Dashboard to the contractor. The CDM Federal Dashboard is operated and maintained outside of this TO.

C.6.2.1 SUBTASK 2.1 – PROVIDE ENGINEERING SUPPORT TO CDM SOLUTION INTEGRATION LAYER

The continuous operation of an Agency's CDM Solution is predicated on the proper functioning of the integration layer (as depicted in Area B of **Diagram 2**). The contractor shall provide engineering support to each Agency's integration layer. At a minimum, the support of the integration layer shall include the following activities:

a. Conduct activities to achieve interoperability between deployed CDM approved products with the integration layer.
b. Provide allowance for the timely and accurate ingestion of data through the integration layer in accordance with Agency standards to ensure the CDM Agency Dashboard data is current.
c. Aggregate CDM tools and sensor data in accordance with Agency processes and procedures in order for the data feeds to output the data to the CDM Agency Dashboard.

d. Conduct activities to ensure data from newly deployed CDM tools and new data feeds are ingested and normalized in the integration layer.
e. Synchronize the desired state communications between the CDM Agency Dashboard and the integration layer in accordance with Agency processes and procedures.
f. Continuously conduct vulnerability assessments of the CDM Solution and:
    1. Inform stakeholders, including Agencies and the DHS TPOC, of remediation of default risk critical/high vulnerabilities in writing.
    2. Identify Agency-focused implementation plan known vulnerabilities that merit Agency patching or remediation upon tool deployment.
    3. Include, at minimum, CVE and CWE-based scan data.

C.6.2.2 SUBTASK 2.2 – CONDUCT TESTING ON CDM SOLUTION

The contractor shall conduct testing on the CDM Solution and new CDM capabilities prior to deployment into operations. Test activities include the development of the test plan, activities, procedures, and results. The CDM Program Test and Evaluation Master Plan (TEMP) (**Section J, Attachment I**) describes the CDM Program planned test and evaluation activities over the Programs' lifecycle and identifies test evaluation criteria. The TEMP is intended to be a living document and, therefore, requires updates to stay current with CDM Program activities and future capabilities. Agency-level TEMPs must remain consistent with the CDM Program TEMP. Approved TEMPs shall be followed throughout the TO performance. The DHS CDM PMO and/or its designated representatives, which may be other contractors, will observe and/or participate in developmental and/or operational tests and evaluations. The Government may conduct additional operational and security-related assessments of the CDM Solution.

The contractor shall conduct testing on CDM solutions by fulfilling the following:

a. Develop a draft and final Agency-Level TEMP (**Section F, Deliverables 29 and 30**) that ensures the delivery of quality CDM capabilities and continued operation of the deployed CDM Solution to the Agencies supported within this TO, update the TEMP to capture changes in the CDM Program TEMP, and test strategy and new capabilities.
b. The TEMP must be inclusive of all testing activities including, at a minimum:
    1. Testing approach:
        i. Critical test parameters
        ii. Evaluation criteria
        iii. Developmental test and evaluation method
        iv. Operational test and evaluation methods for verifying technical and functional requirements
        v. Automated test tools
        vi. Resource management
        vii. A CDM Solution specific Requirements Traceability Matrix (RTM) that is consistent with the template in the DHS CDM Independent Verification and Validation (IV&V) Strategy documentation and clearly identifies any requirements that are disputed, changed, or considered untestable for

CDM PMO adjudication

2. Testing methodologies
    i. Identify the testing tool sets
    ii. Provide a description of the intended test environment
3. Milestone schedules

c. Participate in Test Readiness Reviews (TRRs), which shall be planned at least ten days prior to each test event, and address all items on the TRR checklist (available in the DHS CDM IV&V Strategy documentation).

d. Present the test readiness information to the CDM Test Team for concurrence that all items have been met in order to proceed to the designated Test Milestone/Event. Deliver Test Cases and Test Plans (**Section F, Deliverable 32**) for a particular CDM capability 15 days before a test event. The Test Cases and Test Plans shall include the test and evaluation strategy, test design, test cases, test procedures, and be consistent with the guidance in the DHS CDM IV&V Strategy documentation, including the Sample Test Plan template.

e. Submit a Test Report (**Section F, Deliverable 33**) following each testing event that is consistent with the Test Report Template available in the DHS CDM IV&V Strategy Document (**Section J, Attachment W**).

f. Develop a testing process that ensures all integrated applications are compatible and interoperable with all deployed Agency CDM Solution components prior to installation within the Agency production environment.

g. Conduct test activities for subsequent updates to the CDM Solution, including deployment of new capabilities, and coordinate with the DHS TPOC, and respective Agency representatives for system acceptance.

h. Log and track all test results and problems and make readily available to the DHS TPOC and Agency representatives.

i. Report all major issues that arise from test activities or test results that affect the schedule, and provide recommendations on how to proceed, to the DHS TPOC and Agency representative as soon as it becomes apparent the schedule will be affected.

j. Conduct integration testing activities for the Agency-level CDM Dashboard(s) and the respective CDM Solution.

k. Develop and incorporate the CDM Dashboard integration test activities in the Agency-level TEMP Updates (**Section F, Deliverable 31**) and include, at a minimum:

1. Interface testing
2. Integration testing
3. Performance testing (including stress and load tests)
4. Security testing
5. Accessibility testing
6. Preparation of test plans and procedures
7. Test reports
8. Acceptance testing

l. Conduct end-to-end system testing of the CDM Solution including testing in a test environment and Agency designated environments, which could include development and testing (dev/test), staging, pre-production, and production. End-to-end system testing shall include, at a minimum:
    1. Final acceptance testing of the CDM Solution including CDM Dashboard
    2. Scalability (network performance)
    3. Conducting integration testing of hardware, software, and network
    4. Repeatable processes to accommodate changes in either the CDM Solution or the Agency environment
m. Conduct Post-Implementation Review (PIR) activities to include the following:
    1. Operational testing in the Agency environment
    2. Evaluating effectiveness of incorporating the CDM Solution into the Agency's CDM governance program
n. Participate in the bi-weekly Working-level Integration Product Team (WIPTs) meetings with the CDM Test team and present the status of each Agency's testing activities, test artifacts, test results, concerns, issues or questions, and upcoming testing milestones/event timelines.

C.6.2.3 SUBTASK 2.3 – COORDINATE WITH INDEPENDENT VERIFICATION AND VALIDATION (IV&V) PROVIDER

The contractor shall allow DHS CDM PMO and/or its designated representatives (e.g., IV&V Team) to observe and/or participate in all developmental and/or operational tests and evaluations conducted by the contractor (**Section J, Attachment W**).

The Government may conduct additional operational, security, and accessibility related assessments of the CDM Solution. The contractor shall assist with these assessments as directed by the FEDSIM COR and DHS TPOC.

C.6.2.4 SUBTASK 2.4 – PROVIDE SYSTEMS SECURITY AUTHORIZATION CHANGE MANAGEMENT SUPPORT

The contractor shall ensure the existing CDM Solution at the Agencies maintains system security authorization following the most recent revision of NIST SP 800-37 *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach* and NIST SP 800-53 *Security and Privacy Controls for Federal Information Systems and Organizations*.

In an effort to maintain system security authorization, the contractor shall update the security accreditation package to account for any new CDM capabilities. The Government anticipates activities in this Subtask to only involve updates to a security package, while **Section C.6.4.6** would provide an Agency with a new Security Accreditation Package.

The contractor shall ensure continued integration of the CDM Solution into each Agency's designated Federal Information Standard Management Act (FISMA) inventory system, which in general is categorized as a General Support System (GSS). The security authorization boundary of the CDM Solution shall be treated as a subsystem to the Agency's GSS.

For the purposes of scoping, all CDM Solutions have been categorized for FIPS 199 as High Confidentiality, High Integrity, and Moderate Availability.

The contractor shall provide systems security authorization support by fulfilling the following:

a. Develop documentation to achieve security authorization, in ongoing authorization format, reflecting Agency specific control implementations.
b. Update applicable System Security Plans (SSPs) and Standard Operating Procedures (SOPs).
c. Develop a Security Model and Documentation (**Section F, Deliverable 34**) that updates the applicable Accreditation/Authorization Package, generally in the form of a security control catalog. Provide identification that the security model is the overall security approach to include the catalog of controls.
d. Support Security Test and Evaluation/Security Assessment activities by ensuring availability of the technical team personnel for interviews and artifact collections as required.
e. Create new POA&Ms, update existing POA&Ms, and conduct remediation of findings.
e. Continually integrate the CDM Solution into each Agency's designated FISMA inventory system, which in general is categorized as a GSS.
f. Document changes made to the Agency's CDM Solution in a Security Impact Assessment (**Section F, Deliverable 35**).
g. Conduct vulnerability scans and provide results to Agencies in support of the Agency's Risk Management process and determination, if a reauthorization is required.

A CDM Solution deployed to a cloud environment may be required to meet FEDRAMP requirements. In order to meet FEDRAMP requirements, the contractor may be required to subcontractor with a Third-Party Assessment Organization (3PAO) to perform the necessary security assessment on the cloud CDM Solution to ensure it is fully compliant with FEDRAMP requirements.

C.6.2.5 SUBTASK 2.5 – PROVIDE TIER III SUPPORT TO THE CDM SOLUTION

The contractor shall provide Tier III support to the CDM Solution. Tier III support shall include advanced engineering support to include coordination and resolution with Solution Original Equipment Manufacturers (OEMs). All calls determined by Tier II to be related to the CDM Agency Dashboard and not resolved through Tier II shall be forwarded to the CDM Dashboard provider for Tier III support. Tier III resolution may require after hours support depending on the severity of any identified issues.

C.6.2.6 SUBTASK 2.6 – PROVIDE CDM DASHBOARD TECHNICAL SERVICES

The Government provides iterative releases of the previously installed Agency's CDM Dashboard. The Government's CDM Dashboard provider will provide ongoing support of the CDM Agency Dashboard to the contractor for each release of its CDM Agency Dashboard. The Government's CDM Dashboard provider will train the contractor to install, configure, integrate, and support the CDM Agency Dashboard. The CDM Dashboard provider will maintain and improve the functional processes within CDM Agency Dashboard software.

The Government anticipates between two and three CDM Agency Dashboard releases a year. Typically, CDM Agency Dashboard releases incorporate integration of additional data elements from CDM approved products for CDM Program Phases 1, 2, 3, and beyond. Integration involves mapping CDM tool and sensor data ingested into the integration layer and then mapping the normalized data up to the CDM Agency Dashboard.

For each release of the CDM Agency Dashboard, the Government also anticipates one to three hot fixes that typically incorporate minor changes such as patches for the system components (e.g., RSA Archer platform) and/or bug fixes for summary data feeds to the CDM Federal Dashboard. The level of effort (LOE) to support a hot-fix is typically less than the integration support associated with a Dashboard release.

In support of CDM Agency Dashboard Technical Services, the contractor shall:

a. Install, configure, and maintain each release of the Government-provided CDM Agency Dashboard for use by the Agencies. CDM Agency Dashboards are inclusive of all sub-Agency Dashboards.
b. Conduct quality assurance and technical testing for each release of the delivered CDM Agency Dashboard with respect to its interoperation with the CDM Solution.
c. Ensure that each release of the CDM Agency Dashboard interfaces with the CDM Federal Dashboard.
d. Implement hot-fixes for continued secure operation of the CDM Agency Dashboard.
e. Install, configure, integrate, and transition the CDM Agency Dashboard to production operations.
f. Maintain data input from a single integrated source to the CDM Agency Dashboard.
g. Maintain a CDM data exchange mechanism for the CDM Agency Dashboard and ensure all installed CDM tool and sensor data is sent to the CDM Agency Dashboard.
h. Conduct consistent testing on any changes to the CDM Agency Dashboard.
i. Provide CDM Agency Dashboard testing support and ensure that all installed CDM capabilities report to the CDM Agency Dashboard consistent with Subtask **C.6.2.2**.
j. Ensure new CDM capabilities integrated at each Agency are reported through the CDM Federal Dashboard.

C.6.2.7 SUBTASK 2.7 – PROVIDE AGENCY CDM DASHBOARD TIER II SUPPORT

The contractor shall provide Tier II support to the CDM Agency Dashboard user community including, but not limited to, the following:

a. In-depth troubleshooting.
b. Specialized knowledge of the CDM Solution and CDM Agency Dashboards for remediation.
c. Elevation of all calls determined to be related to the CDM Agency Dashboard and not resolved through Agency CDM Dashboard Tier II support and forwarding of these calls to the CDM Dashboard Provider for Tier III support.

The Agencies will provide the CDM Agency Dashboard Tier I support. CDM Agency Dashboard Tier I support shall include problem resolution using standard methodologies and basic troubleshooting techniques.

C.6.2.8 SUBTASK 2.8 – OPERATE CDM DATA FEEDS

The contractor shall maintain and enhance the CDM data exchange mechanisms, utilizing the Security Content Automation Protocol (SCAP)-compliant Asset Summary Reporting (ASR) Format, as appropriate, between the following:

a. The CDM Solution integration point and CDM Agency Dashboard(s) (Area B and Area C of **Diagram 2**).

b. All CDM Agency Dashboard(s) (within Area C of **Diagram 2**).

c. The CDM Agency Dashboard(s) to the CDM Federal Dashboard - summary level data only (between Area C and Area D of **Diagram 2**).

The contractor shall maintain and enhance data exchange mechanisms that operate between deployed CDM tools and sensors and the CDM Solution's integration layer (between Area A and B of **Diagram 2**).

C.6.3 TASK 3 – INTEGRATE NEW CDM CAPABILITIES

The Government will identify CDM capabilities that require immediate action for implementation of a specific CDM capability or set of capabilities that have not yet been deployed or are requiring updating into an Agency's infrastructure. CDM capabilities are inclusive of filling gaps in an Agency's current CDM environment, expansion of CDM capabilities through new investments, and the technical refresh of previously installed CDM tools and sensors. CDM capabilities are listed below and defined in the CDM Technical Capabilities Requirements Document Volume 1 (**Section J, Attachment Y.1**).

Phase 1: HWAM, SWAM, CM, VUL

Phase 2: TRUST, BEHAVE, CRED, PRIV

Phase 3: BOUND, MNGEVT, OMI, DBS

Phase 4: Micro-segmentation, DRM, Advanced Data Protection

In response to the RFS, the contractor shall provide a technical plan. After Government approval of the technical plan, the contractor shall purchase, install, configure, and customize the CDM capability to ensure proper operation. The contractor shall thoroughly test the CDM capability before transitioning the operation of the capability to an Agency's designated operations team.

C.6.3.1 SUBTASK 3.1 – CDM TECHNICAL PLANNING

In response to the RFS, the contractor shall provide a technical plan defining its approach to implementation of the specific CDM capability or set of capabilities in an Agency's environment. The CDM Technical Planning task shall integrate the contractor's CDM methods and best practices into a sufficiently detailed technical plan, as described in the following subtasks, to ensure successful implementation and operation of the CDM capability at the

Agencies supported by this TO. The plan shall address the need for a CDM capability or solution to be secure and hardened; compliant with typical Federal risk tolerance of zero resident default high, critical vulnerabilities; and configured in a manner consistent with depth and scope of the most recent version of NIST 800-53 control baselines.

C.6.3.1.1 SUBTASK 3.1.1 – VALIDATE CDM CAPABILITY

The validation of a CDM capability consists of two parts:

a. The contractor shall:
    1. Conduct analysis to validate its CDM capability implementation approach against each Agency's existing infrastructure to facilitate CDM Program and IT architecture planning.
    2. Report all discrepancies between information provided by the Government and the existing environments.
    3. Coordinate the analysis with the respective Agencies.
b. The contractor shall develop an Updated Overview of the CDM Capability (**Section F, Deliverable 36**) for inclusion in the Service Design Review (SDR) SELC review, which includes updates as a result of the analysis.

C.6.3.1.2 SUBTASK 3.1.2 – DEVELOP CONCEPT OF OPERATIONS (CONOPS)

The contractor shall develop a CONOPS (**Section F, Deliverable 37**) that describes how the CDM Solution architecture, adjusted for any new CDM capability, shall meet the CDM requirements for the Group E Agencies in their respective environments.

The CONOPS shall include, at a minimum, the following:

a. How the CDM Solution will change as a result of the new CDM capability, specifically identifying how tools associated with the new CDM capability will cover the network and provide data to the integration layer before passing data to the Agency level CDM Dashboard and the Federal Dashboard. The CONOPS shall contain the specifics for the underlying CDM Solution infrastructure and how the infrastructure must change to support any new CDM capability.
b. Methodology to incorporate data into useful information to support operational, tactical, and strategic decisions for Agencies.
c. Methodology to integrate data from the CDM Solution to support decision systems for the Group E Agencies, including managing technical refresh and upgrades of multiple products.
d. Incorporate CDM-specified security configuration settings, as they become available, to the appropriate toolset.
e. How the enhancement of the CDM Solution through the additional CDM capability will provide desired and actual state and the resulting difference or defect information of each Agency endpoint necessary to assist the Agency in defect remediation.

C.6.3.1.3 SUBTASK 3.1.3 – PREPARE CDM SOLUTION/CAPABILITY IMPLEMENTATION ARCHITECTURE

The contractor shall develop an Implementation Architecture and Back-Out Plan (**Section F, Deliverable 38**) that shall include the following, at a minimum:

a. Overview graphical representation of the overall CDM Solution
b. Updates to the CDM Solution that clearly denote the additional CDM capabilities
c. Technical architecture and specifications
d. Data architecture and specifications
e. Interface architecture and specifications
f. Solution functionality
g. High-level functional requirements
h. Operational requirements
i. Plan for reversing implementation, if necessary

The CDM Solution Implementation Architecture shall elaborate how the existing CDM Solution will be enhanced through the new CDM capability. The Architecture shall show the entire solution (including the ABCD layers in **Diagram 2**) and shall show connectivity between and across ABCD.

The contractor shall update the CDM Solution Implementation Architecture as appropriate to reflect As-Built documentation as part of PIR and deliver the CDM Solution Implementation Architecture – As-Built Update (**Section F, Deliverable 39**).

C.6.3.2 SUBTASK 3.2 – INSTALL, CONFIGURE, AND CUSTOMIZE CDM CAPABILITY

Based on the requirements of each Agency, the contractor shall install, configure, and/or customize the tools, sensors, and any supporting ancillary products to meet a CDM capability consistent with the Agency's IT/Network Environment Summary Information, additional information disclosed in **Section C.6.3.1**, and with the IMS and PMP. The contractor shall provide the most current version(s) and release(s) of any and all source, object, executable, and run-time code (as applicable) developed under the efforts of this TO ("New Code") and unique enhancements, customization, and plug-ins, and other similar artifacts ("Customizations") to the Government (**Section F, Deliverable 40**) in accordance with the delivery requirements in **Section F.3**.

The contractor shall design its approach to a CDM capability to ensure that the operating CDM Solution has minimal network performance impact as a result of integrating the CDM capability into the CDM Solution. CDM Technical Capabilities Requirements Documents, Volumes 1 and 2 (**Section J, Attachments Y.1 and Y.2**) define minimal impact as, "Limit the burden put on network resources such that the presence of the scan is not noticeable above background variation in network bandwidth."

It is permissible to include free open source software, free proprietary software, free or priced Government Off-the-Shelf (GOTS) software, or other non-COTS software in the technical plan

for implementing new CDM capabilities within an Agency's CDM Solution, but such software is subject to the Government's approval.

The Government anticipates that no new software development (as opposed to configuration of COTS tools) will be required under this TO. However, in the event that new software development is required, **Section H.17** applies.

C.6.3.3 SUBTASK 3.3 – TRANSITION TO OPERATIONS

After the tools supporting the new CDM capabilities are operational and the solution security authorization has been completed, the contractor shall transition the operation of the solution to the Agency's operations team. The contractor shall provide Agency-designated system administrators full and complete access to the CDM tools and sensors, including their product consoles. The contractor shall be responsible for complete and seamless transition of the overall and Agency-specific solution to each Agency's operations team.

The contractor shall develop a Plan for Transition to Agency Production Operations (**Section F, Deliverable 41**) describing how the contractor shall transition production operations of the modified CDM Solution to the Agency's operations team. The plan for transition to Agency production operations shall include the following elements:

a. Testing Methodology (in support of **Section C.6.2.2**) to include the TEMP.
b. Implementation Methodology, to include the contractor's plan to:
    1. Provide considerations for risk mitigation such as the following:
        i. Demonstration of CDM capability and CDM Solution implementation in lab environment.
        ii. Initial pilot to test the CDM infrastructure with defined success criteria.
        iii. Phased implementation approach.
        iv. User acceptance testing.
        v. Submission of software as part of baseline configuration image.
    2. Roll out of functionality consistent with IMS.
    3. Documentation of Agency Dependencies (**Section F, Deliverable 42**).
    4. Description of configuration management methodology for the tools and sensors of the Agency's CDM Solution.
c. Transition to Agency Operations Team:
    1. Provide training and support to Agency-designated/existing staff to ensure a smooth transition. The training shall be inclusive of the implementation and operation of the specific CDM capability in the Agency's CDM Solution, including the operation of any CDM tools that are implemented to support the CDM capability.
    2. Collect operational requirements needed within the Agencies to operate the solution through the entire life of the TO.
    3. Confirm with Agency Operations Team under the governance of the DHS CDM PMO and the Agencies:
        i. Detailed activities that support the CONOPS

ii. Configuration control
iii. Change control management

The Agency's Production Operations will operate the solution in production after installation and integration in accordance with the Plan for Transition to Agency Production Operations and the IMS.

The contractor shall work in conjunction with the Agency's Production Operations, as well as the FEDSIM COR, DHS TPOC, and the respective Agency, to perform the following:

a. Provide training to the Agency's Production Operations. Provide training and support to Agency-designated/existing staff to ensure a smooth transition.
b. Monitor the solution for system performance and functionality.
c. Incorporate the solution into the respective Agency's continuous monitoring activities.
d. Ensure the solution operates consistent with the Agency system security requirements.
e. Perform problem management in coordination with the Agencies for the solution by identifying problems and performing resolution, to include notifying vendors of application issues. The contractor is expected to continue to provide Tier III (engineering level) support through the POP of the TO in accordance with **C.6.2.5**.
f. Initiate formal requests for any Agency infrastructure modifications and follow change control procedures.

C.6.4 TASK 4 – EXPANDED AGENCY SERVICES (Optional)

Group E Agencies may elect to receive services defined in the following subtasks. The Government anticipates utilizing the RFS process to initiate contractual actions which will execute the subtasks described in detail below.

C.6.4.1 SUBTASK 4.1 – OPERATE AND MAINTAIN CDM SOLUTION

The contractor shall conduct the O&M of the CDM Solution, including the installed suite of CDM tools and sensors. This support may be provided either on-site at the Agency's location(s), from the contractor's facility, from an alternate location, or in combination. While Agency-designated system administrators will have access to the CDM tools and sensors, including their product consoles, the contractor shall be responsible for the operation of the overall CDM Solution. The operational requirements in this task apply to the CDM Solution, to include the Agency CDM Dashboard and associated data feeds, as identified in Areas A, B, and C of **Diagram 2: CDM Architecture** (**Section C.4.1**).

C.6.4.1.1 SUBTASK 4.1.1 – PROVIDE TIER II SUPPORT TO THE CDM SOLUTION

The contractor shall provide Tier II services for the Agency's CDM solution, coordinating with the Agency's and CDM Dashboard Provider's Help Desks. The contractor shall provide hot-line capability during the normal workweek (Monday through Friday) and shall provide coverage from 8:00 a.m. through 6:00 p.m. Eastern Time (ET). In some instances, 24 hours a day and seven day days a week support may be necessary and will be identified in an RFS.

a. The Agencies will provide all Tier I support. Tier I support will include problem resolution using standard methodologies and basic troubleshooting techniques including Agency-raised issues, incident and request management, access and inventory management, change and configuration management, security, and patch management consistent with the Agency's policies and procedures.
b. The contractor shall provide Tier II support for the Agency CDM Solution. Tier II support shall include more in-depth troubleshooting and shall require specialized knowledge of the CDM Solution for remediation.
c. Tier III support to CDM Solution is provided under **C.6.2.5.**

The contractor shall establish a procedure for recording and a ticket tracking mechanism for all operational support requests. On a monthly basis, the contractor shall report the ticket inflow to include the total number of tickets received, types of issues, and how they were resolved in the MSR (**Section C.6.1.3**). The contractor shall, at a minimum, provide the following support:

a. Provide initial problem resolution where possible.
b. Generate, monitor, and track incidents through resolution.
c. Provide software support.
d. Maintain Frequently Asked Questions (FAQs) (**Section F, Deliverable 43**) and their resolutions.
e. Obtain customer feedback and conduct surveys.

C.6.4.1.2 SUBTASK 4.1.2 – PREPARE AND EXECUTE A PLAN FOR PRODUCTION OPERATIONS

The contractor shall develop a Plan for Production Operations (**Section F, Deliverable 44**). The Plan for Production Operations shall describe how the contractor intends to operate the CDM Solution. The Plan for Production Operations shall describe the O&M methodology to supporting the CDM Solution at a particular Agency and shall, at a minimum:

a. Identify requirements needed to operate the CDM Solution through the entire life of the TO.
b. Provide a description of detailed activities that support the CONOPS.
c. Determine data relevant for inclusion in the MSR.
d. Provide a description of the Operational Analysis (**Section F, Deliverable 45**) for PIRs.
e. Describe the configuration management methodology for the tools and sensors of the CDM Solution.
f. Incorporate CDM services on all assets of the Agency's infrastructure, including applications, servers, and desktops.
g. Describe the Change Management methodology for the tools and sensors of the CDM Solution.
h. Incorporate and support Agency specific Service Level Agreements (SLAs).

The contractor shall operate the CDM Solution consistent with the approved Plan for Production Operations. The contractor shall monitor the CDM Solution for system performance and functionality and elevate any issues. The contractor shall incorporate the CDM Solution into the

respective Agency's continuous monitoring activities. The CDM Solution shall operate consistent with the system security requirements. The contractor shall proactively monitor CDM tools for potential disruptions to Agency systems and other security capabilities.

The contractor shall perform problem management in coordination with the Agencies for the CDM Solution by identifying problems and performing resolution, to include notifying OEM vendors of application issues. The contractor shall initiate formal requests for any Agency infrastructure modifications and follow change control procedures. The contractor shall provide technical support for all CDM Solution components and the solution as a whole, whether from a single source or multiple sources.

C.6.4.1.3 SUBTASK 4.1.3 – PERFORM SYSTEM ADMINISTRATION

The contractor shall perform system administration to operate the CDM Solution throughout the TO POP. The contractor shall, at a minimum, provide the following support pending Agency change management approval:

a. Patching
b. Upgrades
c. Replacement of failed components of the CDM Solution

C.6.4.2 SUBTASK 4.2 – PROVIDE GOVERNANCE SUPPORT

Governance is a necessary component for ensuring effective integration of technology into an Agency's cybersecurity program. Agencies are responsible for managing and maintaining cybersecurity specific controls by linking technologies with effective policies and procedures in order to comply with Office of Management and Budget (OMB) guidelines; often described as an Agency's Information Security Continuous Monitoring (ISCM) program.

The contractor shall assist Agencies in incorporating CDM capabilities into each Agency's specific cybersecurity or ISCM program so that the following outcomes are effectively planned, implemented, and documented:

a. Increased and/or more efficient risk-reduction (also described as defect reduction) at Agencies utilizing the most current CDM Agency Dashboard release and supporting technologies.
b. Improved definitions of, or criteria related to, Agency risk-thresholds relative to the CDM architecture and any extant Agency policies or plans related to ISCM.
c. Identification or improved definition of Agency specific "desired states" for use within the CDM architecture in general and current CDM Agency Dashboards and supporting tools in particular, so defect reduction is more effectively or efficiently realized, and Agency machine-level policies for future automated ongoing assessment of current, applicable NIST SP 800-53 controls are met.

C.6.4.2.1 SUBTASK 4.2.1 – ASSESS AND SUPPORT AGENCY CDM GOVERNANCE

The contractor shall deliver a draft and final As-Is Governance Report (**Section F, Deliverable 46**) for each supported Agency. The As-Is Governance Report shall include an analysis of the

current ability of an Agency to leverage CDM information to reduce risk and mitigate defects. The As-Is Governance Report shall also include at a minimum the following:

a. Analysis of any existing Agency-specific Governance Support Plan, as developed during CDM Phase 1 and Phase 2 orders, and how successful the implementation of that Plan has been to support CDM policies.
b. A review of existing ISCM governance structures (charters, policies, memos, procedures, organization structures, and relationships) and how each is utilized in the use of CDM supplied data for risk management activities.
c. A review of Agency workforce planning efforts in the identification and establishment of an information security workforce that supports the use of CDM-supplied data for risk management activities.
d. A review of Agency efforts in planning for the continued support of CDM capabilities and maintenance of an ISCM program.

The contractor shall deliver a draft and final CDM Governance Enhancement Plan (**Section F, Deliverables 47 and 48**) for the Group E Agencies. The CDM Governance Enhancement Plan shall provide the Agency with tailored recommendations and best practices to further enhance the Agency's cybersecurity governance posture; improve Agency-specific CDM governance structures and policies; and establish, modify, improve, and manage each Agency's ISCM Program, with a focus towards risk reduction and defect mitigation. At a minimum, the CDM Governance Enhancement Plan shall include the following:

a. A process to develop or improve and manage Agency-specific ISCM governance structure based on gaps identified in the Governance Assessment Report. This includes identifying any additional policies, procedures, SOPs, and other security documentation that may be required.
b. An approach to integrate CDM capabilities and Federal and Agency-level Dashboard metrics into Agency ISCM or broader cybersecurity governance structures and policies.
c. A strategy to develop, align, or update an Agency's ISCM strategy and approach with federal requirements including but not limited to the following:
    1. OMB M-14-03 *Enhancing the Security of Federal Information and Information Systems*
    2. NIST SP 800-137 *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*
    3. NIST SP 800-37 rev. 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: a Security Life Cycle Approach*
    4. 2016 IG FISMA Metrics, Section 3.0
    5. Current Cross Agency Priority (CAP) Goals for Cybersecurity
d. Tailored recommendations to employ CDM tools beyond CDM requirements to better enable or automate defect reduction, such as:
    1. Tailored best practice guidelines on utilizing applicable CDM tools to perform network access control to minimize HWAM defects from negatively impacting Agency risk thresholds and metrics.

2. Further automation of previously manual cybersecurity controls or capabilities through use of the CDM tools and architecture and suggestions of how better to utilize cyber staff as a result.
3. Furthering support of Application Whitelisting (AWL) via applicable CDM tools, tailored to Agency process and structure and degree of federation, so that defect-reducing outcomes described above are supported.
4. Orchestration with existing service desk ticketing and/or network monitoring systems.
5. Use of authoritative HWAM asset data for streamlined FISMA boundary delta updates to incorporate relevant stakeholders.
6. Expansion of CDM tool functionality to consider inclusion of development networks and development oversight.

e. Identification of any additional support to further expand governance support required to support each Agency's CISO.

The contractor shall host bi-weekly Inter-Agency governance coordination meetings. The contractor shall maintain invitations and continuously solicit participation for the appropriate stakeholders based on meeting topics. The contractor shall lead the meeting and maintain the meeting agenda, a repository of meeting summaries, and a repository of lessons learned (**Section F.3, Deliverable 11**).

In addition, the contractor shall host CDM working groups at each individual Agency as needed to focus on prioritizing and addressing any suggested governance updates.

C.6.4.2.2 SUBTASK 4.2.2 – DEVELOP AND UPDATE ISCM GOVERNANCE DOCTRINE

Agencies will execute additional governance support as needed to fill identified gaps in existing security doctrine.

Based on the approved CDM Governance Support, the contractor shall develop and deliver CDM Governance Documentation (**Section F, Deliverable 49**) that shall assist Agencies with strengthening security programs through additional controls. CDM Governance Documentation shall consist of, but is not limited to, the following:

a. SOPs
b. Policy
c. Procedures
d. Directives

The contractor shall deliver a CDM Communications Plan (**Section F, Deliverable 50**), which shall assist Agencies with managing internal communication efforts related to CDM. At a minimum, the CDM Communications Plan shall include the following:

a. A strategy to increase effectiveness of internal CDM activities
b. A communications approach for varying audiences depending on CDM impacts
c. A roadmap for continued communication

C.6.4.3 SUBTASK 4.3 – PROVIDE CDM SOLUTION TRAINING

The contractor shall provide training on implementation and operation of an Agency's CDM Solution, including the operation of individual CDM tools.

The contractor training shall deliver CDM Solution Training Plan Documentation (**Section F, Deliverable 51**) consisting of all training materials, any training manuals, COTS manuals for all installed CDM-related tools, and a Training Plan for each Group E Agency. At a minimum, the Training Plan shall include the following:

a. Training method
b. Training medium
c. Training tools
d. Frequency of training
e. Audience
f. Location
g. Method to incorporate training feedback

The contractor shall ensure all training is consistent with the DHS-provided CDM Program training content. The DHS CDM training content provides an overview of CDM concepts, principles, and approaches for all phases of the CDM Program and how CDM capabilities work together.

At a minimum, the contractor shall deliver the following CDM Solution-based training:

a. **CDM Solution Overview Training**. The contractor shall conduct this training prior to deploying new CDM capabilities in an Agency's CDM environment. This training shall include detailed information on how the Agency can operationalize CDM Dashboard metrics.
b. **CDM Solution Technical Training**. The contractor shall provide training on the CDM Solution product configuration, integration, and operations as they relate to an Agency's network environment. This training is not intended to replace manufacturer's certification training. This training shall be role-based and consist of two subsets of training, specifically:
    1. CDM Tools-specific hands-on training for the user community, which allows the end-user to experience operations and the use of specific tools at the Agency, including vendor based product training. This training can be provided at a contractor facility, virtually, or at the Agency site.
    2. Scenario-based training that exposes users to real-world use of the entire CDM Solution. This training can be provided at a contractor facility, virtually, or at the Agency site.
c. **CDM Agency Dashboard Technical Training**. This training shall include hands-on training on how certain users can operate the delivered Agency Dashboard.

The CDM Agency and Federal Dashboard provider will provide standardized FOC CDM Dashboard training materials to the contractor when delivering the CDM Agency Dashboard training. The contractor shall present content specific to the CDM Solution as it relates to the

standardized CDM Agency Dashboard training content with consideration of Agency unique environments.

C.6.4.4 SUBTASK 4.4 – PROVIDE CDM ASSET MANAGEMENT TRACKING

The contractor shall track IT assets leveraging IT asset information gained through the CDM Phase 1 implementation and shall assist the Agency with efforts to centralize IT license management. The contractor shall recommend strategies and practices that reduce duplicative IT purchases and streamline the purchase of maintenance on existing IT investments. The contractor shall institute processes that alert Agency representatives of funding requirements for the continuing maintenance of the IT investments.

In addition, the contractor shall provide an Agency-Specific Software License Inventory (**Section F, Deliverable 53**), including all licenses purchased, deployed, and in use, as well as spending on subscription services, to include provisional (i.e., cloud) Software as a Service (SaaS) agreements. The contractor shall analyze inventory data to ensure compliance with software license agreements, consolidate redundant applications, and identify other cost-saving opportunities.

C.6.4.5 SUBTASK 4.5 – INTEGRATE AGENCY DATA AND APPLICATION INTO THE CDM SOLUTION

Agencies may have applications that require integration into the CDM Solution for the purposes of data sharing. The contractor shall integrate and maintain interoperability between the CDM Solution and other Agency legacy applications for the purpose of sharing data.

The contractor shall establish the data exchange mechanism between the CDM Solution and Agency applications that hold the necessary information. Examples of applications include, but are not limited to, the following:

a. Discovery tools
b. Network asset systems (e.g., Active Directory and other Lightweight Directory Access Protocol (LDAP)-like systems)
c. Property management systems
d. Configuration management systems
e. Vulnerability management systems
f. Open Checklist Interactive Language (OCIL) questionnaire systems

The contractor shall periodically perform the appropriate data exchanges between the Agency legacy applications and the CDM Solution to ensure the CDM Solution uses the most current data as defined by the Agency policy. The contractor shall update the data exchange mechanism in response to changes in either the Agency applications or the CDM Solution.

C.6.4.6 SUBTASK 4.6 – PROVIDE SYSTEMS SECURITY AUTHORIZATION SUPPORT

The contractor shall provide System Security Authorization support to develop new or replacement security accreditation packages for the deployed CDM Solution.

In accordance with the FISMA, the CDM Solution at each Agency is required to receive/maintain system security authorization following the most recent version of NIST SP 800-37 *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach* and NIST SP 800-53 *Security and Privacy Controls for Federal Information Systems and Organizations*.

The contractor shall support the Agency's System Accreditation and on-going authorization processes and activities to ensure that the implementation of the security controls maintain effectiveness over time. These activities include, but are not limited to, the following:

a. Provide the Agencies with new or replacement documentation to support the Agencies' security authorization (in ongoing authorization format). This includes control implementation updates in applicable SSPs and SOP updates as applicable.
b. Provide technical support to the Agency's security authorization process related to the CDM Solution:
    1. Support Security Test and Evaluation/Security Assessment activities by ensuring availability of the technical team personnel for interviews and artifact collections as required.
    2. POA&M Management
        i. Remediation and updates to existing POA&Ms
        ii. Creation of new POA&Ms

Any portion of an Agency's CDM solution that is deployed and resides in a cloud environment may be required to meet FEDRAMP requirements. In order to meet FEDRAMP requirements, the contractor may be required to subcontract with a 3PAO to perform the necessary security assessment on a specific CDM cloud solution to ensure it is fully compliant with FEDRAMP requirements.

C.6.4.7 SUBTASK 4.7 – PROVIDE CONTINUOUS AGENCY ISCM STRATEGIC AND CIO/CISO PROGRAMMATIC SUPPORT

Each Agency will consider longer term strategic objectives of their ISCM programs and how CDM can be leveraged to support the achievement of those objectives. Agencies will require additional programmatic support to assist in the establishment and transformation of CISO and CIO program offices to support the strategic direction of the Agency's ISCM program.

The contractor shall provide support for this process that consists of:

a. Establishing and transforming CIO and CISO program offices that leverage CDM capabilities to meet strategic objective and inform data-driven decision making to reduce Agency cyber risk.
b. Developing policies, processes, and procedures that support the operationalization of:
    1. Security objectives outlined in the Agency's ISCM Strategy.
    2. Federal policies, regulations, guidelines, and standards.
c. Developing, implementing, and operating a configuration management approach that aligns with the capabilities provided by the CDM Solution.
d. Development, implementation, and operation of a knowledge management approach.

C.6.5 TASK 5 – SURGE CYBERSECURITY CRITICAL INCIDENT SUPPORT (Optional)

The Government anticipates surge support will be required on a case-by-case basis when Agencies supported by this TO are impacted by cyber-attacks, in need of penetration testing, or require cyber risk assessment and mitigation activities. The scope of the response shall consist of conducting an initial assessment of the attack, identifying a plan of action, and implementing the approved response.

The Government plans to initiate surge support services using the RFS process (**Section C.5**). The Government will provide the requirements for the timing of the contractor's response upon initiating the support. Surge support shall not result in a decrease of support to other TO requirements unless approved by the FEDSIM CO and FEDSIM COR.

The following applies to performing the cyber-attack surge support:

a. The Government will estimate the scope of surge support required at the time of the cyber-attack.
b. The contractor may be required to provide surge support at Agency spaces.
c. Once a cyber-attack response has ended, the contractor shall proceed with an orderly and efficient transition-out period. During the transition-out period, the contractor shall fully cooperate with, and assist the Government with, activities closing out the matter, developing required documentation, transferring knowledge, training, and lessons learned.